Studiu empiric al rețelei de anonimitate I2P și al rezistenței sale la cenzură

Nguyen Phong Hoang
Universitatea Stony Brook, Stony Brook, New York
nghoang@cs.stonybrook.edu

Panagiotis Kintis
Georgia Institute of Technology, Atlanta, Georgia
kintis@gatech.edu

Manos Antonakakis
Georgia Institute of Technology, Atlanta, Georgia
manos@gatech.edu

Michalis Polychronakis
Universitatea Stony Brook, Stony Brook, New York
mikepo@cs.stonybrook.edu

2018; © ACM

REZUMAT

Tor și I2P sunt rețele de anonimitate bine cunoscute, utilizate de numeroși oameni pentru a-și proteja confidențialitatea și anonimatul online. Serviciile centralizate de directoare ale Tor facilitează înțelegerea rețelei Tor, precum și măsurarea și vizualizarea structurii sale prin proiectul Tor Metrics. În schimb, I2P nu se bazează pe servere centralizate de directoare, ceea ce face dificilă obținerea unei imagini complete a rețelei.

În această lucrare realizăm un studiu empiric al rețelei I2P, în cadrul căruia măsurăm caracteristici precum dimensiunea rețelei, rata de fluctuație a nodurilor, tipurile de routere și distribuția geografică a participanților I2P. Am constatat că în prezent există aproximativ 32.000 de participanți I2P activi zilnic. Dintre aceștia, aproximativ 14.000 se află în spatele unor dispozitive NAT sau al unor firewall-uri.

Folosind datele colectate din rețea, analizăm rezistența I2P la blocare în fața unui cenzor care dorește să împiedice accesul la I2P prin tehnici de blocare bazate pe adrese. În ciuda caracterului descentralizat al I2P, descoperim că un cenzor poate bloca peste 95% dintre adresele IP ale participanților cunoscuți de un client I2P stabil operând doar 10 routere în rețea. Acest lucru conduce la o

degradare severă a funcționării rețelei: o rată de blocare de peste 70% este suficientă pentru a provoca întârzieri semnificative în navigarea web, iar blocarea a peste 90% dintre adresele IP ale participanților poate face rețeaua inutilizabilă. În final, discutăm consecințele de securitate ale blocării rețelei și posibile direcții pentru creșterea rezistenței I2P la astfel de măsuri.

Cuvinte-cheie:
Rețea de anonimitate I2P, metrici de rețea, cenzura Internetului, rezistență la blocare

1. INTRODUCERE

În ultimii ani, cenzura și supravegherea Internetului au devenit fenomene tot mai răspândite. Din acest motiv, comunicațiile anonime au atras atenția atât a cercetătorilor, cât și a utilizatorilor de Internet. Pe măsură ce rețelele de comunicații anonime ajung să deservească tot mai mulți utilizatori, devin disponibile gratuit din ce în ce mai multe instrumente pentru protejarea anonimatului și evitarea cenzurii. Printre acestea se numără serverele proxy, serviciile Virtual Private Network (VPN), Onion Router (Tor) și Invisible Internet Project (I2P). Tor și I2P sunt cele mai populare rețele de comunicații anonime cu latență redusă, care folosesc tehnica rutării onion pentru a proteja anonimatul utilizatorilor.

Deși Tor și I2P oferă funcționalități similare, există câteva diferențe importante între ele. Tor operează la nivelul fluxurilor TCP,

în timp ce traficul I2P poate utiliza atât TCP, cât și UDP. Tor are o arhitectură centralizată, în care un grup de autorități de directoare monitorizează rețeaua, pe când, din cauza naturii sale descentralizate, nicio entitate nu deține o imagine completă asupra rețelei I2P. Fiecare participant I2P contribuie implicit la rutarea traficului altor participanți, în timp ce în mai 2018 existau doar aproximativ 6.500 de routere Tor care deserveau peste două milioane de utilizatori zilnic. Ca urmare, Tor este conceput în principal pentru activități sensibile la latență, precum navigarea web, din cauza limitărilor de lățime de bandă, în timp ce capacitatea I2P permite și utilizarea unor aplicații peer-to-peer (P2P) cu consum ridicat de trafic, cum ar fi BitTorrent.

Pe lângă posibilitatea navigării anonime pe Internet, aceste rețele oferă și servicii ascunse, care alcătuiesc așa-numitul „dark web”, unde anonimatul atât al expeditorilor, cât și al destinatarilor este păstrat, protejând astfel viața privată a utilizatorilor. Datorită popularității sale și sprijinului oferit de nodurile de ieșire operate de voluntari către Internetul obișnuit, Tor a fost utilizat pe scară largă și studiat intens. În schimb, I2P nu a beneficiat de aceeași atenție din partea comunității de cercetare.

Identificăm două motive posibile pentru care rețeaua I2P a fost mai puțin atractivă decât Tor. În primul rând, arhitectura complet distribuită a I2P, lipsită de orice serviciu centralizat de directoare, este mult mai dificil de măsurat. În al doilea rând, disponibilitatea intermitentă a nodurilor de ieșire face ca I2P să funcționeze, în cea mai mare parte a timpului, ca o rețea autonomă care deservește doar servicii ascunse, fiind astfel mai puțin atractivă pentru utilizatorii care doresc să navigheze ocazional pe Internetul public.

În această lucrare ne propunem să reducem acest deficit de cercetare prin realizarea unei măsurători empirice a rețelei I2P. Considerăm că aceasta poate contribui atât la popularizarea I2P în rândul cercetătorilor și al utilizatorilor de Internet, cât și la o mai bună înțelegere a structurii și proprietăților sale. Având în vedere aceste obiective, studiul nostru urmărește să răspundă la următoarele întrebări principale.

Care este dimensiunea populației de participanți I2P din rețea?

În timp ce Tor se bazează pe o arhitectură centralizată pentru monitorizarea releelor publice, indexate de un set de servere de autoritate predefinite, I2P este o rețea P2P distribuită în care nicio autoritate centrală nu poate urmări toți participanții activi. Dezvoltatorii Tor pot colecta cu ușurință informații despre rețea și chiar o pot vizualiza, prin intermediul proiectului Tor Metrics. În schimb, foarte puține studii au încercat să măsoare rețeaua I2P.

În această lucrare încercăm să estimăm dimensiunea rețelei I2P prin operarea a până la 40 de noduri I2P configurate diferit în scopuri de monitorizare. Rezultatele arată că în prezent există aproximativ 32.000 de participanți I2P activi zilnic. Statele Unite, Rusia, Anglia, Franța, Canada și Australia reprezintă peste 40% dintre acești participanți. Spre deosebire de lucrările anterioare, am observat și aproximativ 6.000 de participanți proveniți din 30 de țări cu scoruri reduse privind libertatea presei. Acest lucru sugerează că I2P este posibil să fie utilizată ca alternativă la Tor în regiuni caracterizate prin cenzură și supraveghere intensă a Internetului.

În ce măsură este I2P rezistentă la cenzură și care este costul blocării sale?

În ciuda existenței numeroaselor instrumente orientate spre protejarea confidențialității și combaterea cenzurii, acestea sunt adesea blocate cu ușurință de autoritățile locale, devenind inaccesibile sau dificil de utilizat pentru persoanele fără cunoștințe tehnice avansate. Din acest motiv, nu este suficientă doar dezvoltarea unor instrumente de comunicație rezistente la cenzură; ele trebuie să rămână și ușor accesibile utilizatorilor finali.

Din cauza naturii centralizate a arhitecturii Tor, un cenzor poate obține relativ ușor o listă cu toate routerele Tor publice și le poate bloca. Chiar și routerele ascunse, cunoscute și sub numele de „bridges”, sunt adesea descoperite și blocate. În ciuda designului său descentralizat, au fost raportate și tentative de blocare a I2P. Totuși, după cunoștințele noastre, niciun studiu anterior nu a analizat cât de dificil este pentru un cenzor să blocheze accesul la I2P.

Analizând datele colectate despre rețeaua I2P, evaluăm rezistența sa la cenzură folosind un model probabilistic. Descoperim că un cenzor poate bloca peste 95% dintre adresele IP ale participanților cunoscuți de un client I2P stabil prin introducerea în rețea a doar 10 routere.

Pe scurt, contribuția principală a acestei lucrări constă într-o evaluare empirică a rețelei I2P, menită atât să îmbunătățească înțelegerea proprietăților sale, cât și să evalueze vulnerabilitatea rețelei la blocarea bazată pe adrese.

Restul articolului este organizat după cum urmează. Secțiunea 2 oferă informații generale despre I2P și prezintă lucrările conexe. Considerațiile etice, parte indispensabilă a oricărui studiu asupra unei rețele de anonimizare, sunt discutate în Secțiunea 3, unde justificăm principiile pe care le-am urmat în colectarea și analiza

datelor. În Secțiunea 4 explicăm metodologia de măsurare, inclusiv specificațiile sistemelor utilizate, lățimea de bandă disponibilă și tipurile de routere I2P folosite în experimente. Rezultatele măsurătorilor privind proprietățile rețelei I2P, precum numărul de participanți, rata de fluctuație și distribuția acestora, sunt analizate în Secțiunea 5. Pe baza acestor caracteristici, evaluăm apoi rezistența la blocare a rețelei în Secțiunea 6, unde constatăm că I2P este foarte vulnerabilă la blocarea bazată pe adrese, în pofida naturii sale descentralizate. În final, în Secțiunile 7 și 8 discutăm consecințele cenzurării rețelei și prezentăm posibile soluții pentru îngreunarea tentativelor de blocare a I2P bazate pe adrese, pornind de la concluziile obținute în urma măsurătorilor noastre asupra rețelei.

2. CONTEXT ȘI LUCRĂRI CONEXE

2.1. I2P: The Invisible Internet Project

2.1.1. Mecanismul de rutare

Invisible Internet Project (I2P) este o rețea anonimă de retransmisie orientată pe mesaje, alcătuită din participanți (numiți și noduri, relee sau routere) care rulează software-ul I2P Router, permițându-le să comunice între ei.

În timp ce Tor utilizează circuite bidirecționale bazate pe rutarea *onion* pentru comunicare, I2P folosește tuneluri unidirecționale bazate pe rutarea *garlic* pentru mesajele de intrare și de ieșire. Un client I2P utilizează două tipuri de tuneluri de comunicație: inbound (intrări) și outbound (ieșiri). Din acest motiv,

pentru o singură cerere transmisă între două părți și răspunsul aferent sunt necesare patru tuneluri, după cum este ilustrat în Figura 1. Pentru simplitate, fiecare tunel este reprezentat cu două salturi (*hops*). În practică, în funcție de nivelul de anonimitate dorit, tunelurile pot fi configurate să conțină până la șapte salturi. Tuneluri noi sunt create la fiecare zece minute.

Când Alice dorește să comunice cu Bob, ea trimite mesaje prin tunelul său de ieșire (*outbound*). Aceste mesaje sunt direcționate către routerul-gateway al tunelului de intrare (*inbound*) al lui Bob. Alice află adresa routerului-gateway al lui Bob prin interogarea unei baze de date distribuite a rețelei (discutată mai detaliat în Secțiunea 2.1.2). Pentru a-i răspunde lui Alice, Bob urmează același proces și trimite mesajele de răspuns prin propriul tunel de ieșire către gateway-ul tunelului de intrare al lui Alice. Anonimatul ambilor participanți este păstrat deoarece fiecare cunoaște doar adresele gateway-urilor, nu și adresele reale ale celuilalt. Trebuie remarcat faptul că gateway-urile tunelurilor de intrare sunt publicate, în timp ce gateway-urile tunelurilor de ieșire sunt cunoscute exclusiv de utilizatorul care le folosește.

Exemplul din Figura 1 ilustrează o situație în care I2P este utilizată ca rețea autonomă, participanții comunicând exclusiv între ei. Dacă Bob oferă și un serviciu de outproxy, Alice își poate redirecționa traficul prin Bob pentru a accesa Internetul public. Traficul de răspuns este apoi retransmis în siguranță către Alice prin tunelurile de ieșire ale lui Bob, în timp ce identitatea lui Alice rămâne necunoscută atât pentru Bob, cât și pentru destinația accesată pe Internet.

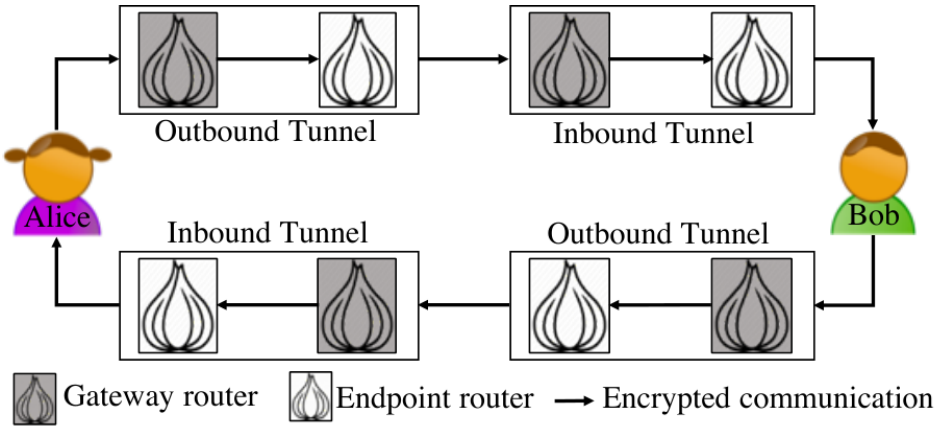

Figura 1. Comunicarea de bază între doi utilizatori I2P
prin intermediul tunelurilor unidirecționale (Pagina oficială I2P, 2017).

Similar rutării *onion* utilizate de Tor, atunci când un mesaj I2P este transmis printr-un tunel (de la gateway la capătul acelui tunel), acesta este criptat de mai multe ori de către expeditor folosind cheile publice ale salturilor selectate. Fiecare nod intermediar elimină un strat de criptare pentru a afla adresa următorului nod către care trebuie retransmis mesajul.

Când mesajul trece printr-o interconectare între tuneluri (adică dintr-un tunel de ieșire într-un tunel de intrare), expeditorul utilizează criptarea *garlic* (ElGamal/AES), adăugând un strat suplimentar de criptare la capete pentru a ascunde conținutul mesajului atât față de nodul final al tunelului de ieșire, cât și față de gateway-ul tunelului de intrare.

Spre deosebire de Tor, mai multe mesaje pot fi grupate într-un singur mesaj *garlic* I2P. Odată dezvăluite la capătul tunelului de transmisie, fiecare dintre aceste mesaje, denumite **„bulb”** (sau **„clove”** în terminologia I2P), conține propriile instrucțiuni de livrare.

O altă diferență majoră între Tor și I2P este faptul că toate nodurile I2P (cu excepția routerelor ascunse, discutate în

Secțiunea 5.1) participă și ca relee în rețea, rutând trafic pentru alte noduri. În Figura 1, salturile (reprezentate prin simboluri de tip ceapă încadrate într-un chenar) care formează tunelurile lui Alice și Bob corespund unor utilizatori reali ai rețelei I2P.

În timp ce retransmit mesaje pentru Alice și Bob, aceste noduri pot comunica simultan și cu propriile destinații, la fel cum fac Alice și Bob. În mod similar, Alice și Bob pot fi selectați de alți participanți pentru a lua parte la tunelurile pe care aceștia le construiesc.

2.1.2. Distribuiția directoarelor

Baza de date a rețelei I2P, denumită **netDb**, joacă un rol esențial în funcționarea rețelei, permițând participanților să interogheze informații despre alți participanți și despre serviciile ascunse. Această bază de date este implementată sub forma unui tabel hash distribuit (*Distributed Hash Table – DHT*), utilizând o variantă a algoritmului Kademlia.

Atunci când un nou participant se conectează la rețea, acesta învață inițial doar o mică parte din conținutul netDb printr-un proces de inițializare (*bootstrapping*), descărcând informații despre alți participanți din rețea de la un set de servere *reseed* preconfigurate. Spre deosebire de directoarele din Tor, aceste servere *reseed* nu dețin o imagine completă a întregii rețele I2P. Ele sunt echivalente cu orice alt participant din rețea, având doar capacitatea suplimentară de a furniza noilor participanți o mică parte dintre routerele cunoscute.

Interogările către baza de date a rețelei sunt procesate de un grup special de routere numite **floodfill**. Acestea joacă un rol esențial în menținerea **netDb**. Una dintre principalele lor

responsabilități este stocarea descentralizată a informațiilor despre participanți și serviciile ascunse prin intermediul unor chei de indexare (adică chei de rutare).

Aceste chei sunt calculate prin aplicarea funcției hash SHA-256 asupra unei chei binare de căutare de 32 de octeți, concatenată cu un șir care conține data UTC. Ca urmare, valorile **hash** rezultate se modifică zilnic, la ora 00:00 UTC.

În arhitectura actuală a I2P există două modalități de a deveni router **floodfill**. Prima constă în activarea manuală a modului ***floodfill*** din consola routerului I2P. A doua posibilitate este ca un router cu lățime mare de bandă să devină automat router ***floodfill*** după ce trece o serie de teste de „sănătate”, precum stabilitatea și timpul de funcționare în rețea, debitul cozii de mesaje de ieșire, latența și alte criterii similare.

Baza de date **netDb** conține două tipuri de metadate de rețea: **LeaseSets** și **RouterInfos**.

De exemplu, *LeaseSet*-ul lui Bob îi furnizează lui Alice informațiile de contact ale gateway-ului tunelului de intrare al lui Bob. Un obiect **RouterInfo** conține informații de contact despre un anumit participant I2P, inclusiv cheia sa criptografică, capacitatea, adresa și portul utilizat.

Pentru a-și publica *LeaseSet*-urile, Bob trimite un mesaj DatabaseStoreMessage (DSM) către mai multe routere ***floodfill***. Acest mesaj conține *LeaseSet*-urile sale.

Pentru a obține informațiile din *LeaseSet*-ul lui Bob, Alice trimite un mesaj DatabaseLookupMessage (DLM) către acele routere *floodfill*.

2.2. Lucrări conexe
2.2.1. Măsurarea rețelei I2P

Înaintea acestei lucrări, au existat doar câteva studii dedicate monitorizării rețelei I2P.

În 2011, Timpanaro și colaboratorii au construit o arhitectură de monitorizare pe infrastructura experimentală PlanetLab pentru a caracteriza modul de utilizare a rețelei I2P. PlanetLab este o rețea alcătuită din noduri voluntare operate de institute de cercetare și universități din întreaga lume. Din acest motiv, politicile privind lățimea de bandă și traficul aplicate nodurilor din această rețea sunt adesea restrictive. După cum au recunoscut autorii, din cauza limitărilor impuse asupra lățimii de bandă disponibile în PlanetLab, au putut configura cu succes doar 15 routere **floodfill**, ceea ce a limitat volumul de date colectate. Ulterior, autorii și-au extins cercetările pentru a caracteriza utilizarea rețelei I2P, în special folosirea aplicațiilor de partajare a fișierelor în cadrul acesteia.

În 2014, Liu și colaboratorii au raportat că au putut observa 25.640 de participanți pe zi, pe o perioadă de două săptămâni, utilizând diverse metode pentru descoperirea topologiei rețelei. Totuși, metodologia folosită de aceștia pentru colectarea informațiilor de tip **RouterInfo** prezintă anumite probleme, pe care le vom discuta în secțiunile următoare ale acestei lucrări.

Mai recent, Jeong și colaboratorii au raportat scurgeri ale interogărilor de rezolvare a numelor de domeniu **.i2p** în infrastructura DNS publică. Rusia, Statele Unite și China se numără printre principalele surse ale acestor scurgeri. Gao și colaboratorii au realizat un studiu privind popularitatea și disponibilitatea **eepsites**-urilor (termenul utilizat în I2P pentru site-urile web anonime). Autorii au susținut că au identificat 1.861 de

eepsites active, care reprezentau peste 80% din totalul site-urilor anonime existente în rețeaua I2P.

2.2.2. Blocarea rețelelor de comunicații anonime

Din câte știm, nu au existat până acum lucrări care să se concentreze asupra rezistenței I2P la blocare. Prin această lucrare ne propunem să aducem mai multă claritate asupra acestui aspect al rețelei. La fel ca Tor sau orice altă rețea anonimă, I2P este vulnerabilă la blocare. Înaintea acestui studiu au existat câteva produse comerciale care pretindeau că pot bloca traficul I2P. Totuși, din câte am putut constata, în pofida diverselor tehnici utilizate, niciunul dintre aceste instrumente nu poate bloca I2P în mod eficient, sau cel puțin nu la nivelul necesar pentru implementarea unei cenzuri pe scară largă, cum ar fi blocarea la nivel național. În continuare analizăm pe scurt câteva dintre aceste soluții.

În administrarea rețelelor, regulile de firewall sunt utilizate frecvent pentru a permite sau filtra traficul. Cele mai răspândite tehnici de blocare se bazează pe numărul portului, semnătura protocolului sau adresa IP. Rețelele de anonimitate, inclusiv Tor și I2P, sunt concepute pentru a rezista cenzurii. Din acest motiv, orice încercare de blocare a acestora poate provoca efecte colaterale considerabile.

În cazul cenzurii bazate pe porturi, blocarea porturilor releelor Tor (*orports*) sau a porturilor utilizate pentru schimbul informațiilor de director (*dirports*) este suficientă pentru a bloca releele Tor. În mod similar, blocarea portului UDP 123 ar împiedica funcționarea corectă a I2P, deoarece software-ul routerului I2P depinde de

serviciul Network Time Protocol (NTP). Cu toate acestea, multe relee Tor utilizează porturile 80 (HTTP) sau 443 (HTTPS) pentru *orports* și *dirports*, iar numeroase aplicații legitime folosesc, la rândul lor, portul 123 pentru NTP.

În plus, I2P este o aplicație P2P care poate funcționa pe o gamă largă de porturi, folosind atât UDP, cât și TCP. Mai precis, I2P poate rula pe orice port din intervalul 9000-31000. Din această cauză, blocarea porturilor nu reprezintă o soluție ideală pentru cenzura la scară largă, deoarece poate bloca accidental și traficul altor aplicații legitime.

Pe măsură ce cenzura Internetului la nivel național se extinde în tot mai multe regiuni ale lumii, tehnologia **Deep Packet Inspection (DPI)** este utilizată pe scară largă pentru identificarea modelelor de trafic asociate **conexiunilor către rețelele de anonimitate.** Indiferent dacă folosesc porturi consacrate, precum 80 sau 443, conexiunile către releele de intrare Tor pot fi identificate prin amprentare și blocate cu ușurință de firewall-uri echipate cu DPI.

Pentru a contracara acest lucru, comunitatea Tor a introdus mecanismele cunoscute sub numele de **pluggable transports**. Acestea fac ca traficul dintre client și nodurile *bridge* Tor să semene cu alte tipuri de trafic obișnuit și răspândit pe Internet.

În mod similar, designul I2P include mecanisme de ofuscare a traficului pentru a împiedica identificarea protocolului pe baza analizei conținutului pachetelor. Totuși, în configurația actuală, analiza fluxurilor de trafic (*flow analysis*) poate fi folosită pentru identificarea traficului I2P, deoarece primele patru mesaje ale procesului de stabilire a conexiunii dintre routerele I2P au dimensiuni fixe de 288, 304, 448 și 48 de octeți. Pentru a rezolva

această problemă, echipa I2P lucrează la dezvoltarea unui protocol autentificat de negociere a cheilor, conceput să reziste diferitelor forme de identificare automată și altor tipuri de atacuri.

Tenable, o companie specializată în securitatea rețelelor, oferă un serviciu de firewall care include module pentru detectarea traficului I2P. Analiza documentației lor ne-a arătat că niciuna dintre metodele propuse nu pare suficient de eficientă pentru blocarea I2P. De exemplu, una dintre recomandările pentru detectarea traficului I2P de ieșire constă în inspectarea manuală a sistemului în căutarea unor procese suspecte. O astfel de abordare este dificil de aplicat într-un scenariu de blocare la scară largă, cum ar fi cenzura națională.

SonicWALL, companie specializată în controlul conținutului și securitatea rețelelor, recomandă blocarea I2P prin filtrarea atât a traficului UDP, cât și a celui TCP asociat tunelurilor, utilizând funcționalitatea App Control pentru a împiedica accesul prin proxy. Nici această abordare nu este practică la scară mare. Chiar compania recunoaște că metoda poate produce efecte colaterale importante, blocând involuntar și alte tipuri de trafic legitim, precum traficul UDP criptat, conexiunile IPSec VPN sau alte comunicații TCP criptate.

O abordare mai eficientă este filtrarea bazată pe destinație. Pentru a o implementa, un cenzor trebuie să compileze o listă a adreselor participanților I2P activi și să blocheze accesul către toate acestea. O astfel de metodă de blocare bazată pe adrese ar afecta grav procesul de construire a noilor tuneluri I2P și, implicit, ar împiedica utilizatorii să acceseze rețeaua.

Există și o metodă mai simplă, dar în continuare eficientă, pentru a împiedica noii utilizatori să se conecteze la I2P: blocarea

accesului la serverele reseed, indispensabile procesului de inițializare (*bootstrapping*). În aceste condiții, utilizatorii care se conectează pentru prima dată nu vor putea accesa rețeaua I2P dacă nu pot descărca informațiile RouterInfo ale altor participanți.

Pentru a face față acestei probleme, I2P oferă o metodă de *reseed* manual al routerelor, pe care o discutăm în Secțiunea 6.1.

Unul dintre obiectivele principale ale cercetării noastre este evaluarea costului și eficienței blocării bazate pe adrese în cazul rețelei I2P.

3. Considerații etice

Desfășurarea cercetării asupra unor rețele de anonimitate care cuprind mii de utilizatori trebuie realizată într-un mod responsabil, care să respecte atât confidențialitatea utilizatorilor, cât și buna funcționare a rețelei. Acest lucru impune și gestionarea cu maximă atenție a tuturor datelor colectate.

Deși routerele I2P sunt operate de persoane care pot utiliza activ rețeaua în scopuri proprii, studiul nostru nu implică cercetare pe subiecți umani, deoarece se concentrează exclusiv asupra infrastructurii furnizate de I2P. Măsurătorile noastre nu captează traficul utilizatorilor și nici activitățile lor online. Analizăm exclusiv caracteristicile rețelei la nivel de infrastructură.

Pentru realizarea măsurătorilor noastre, a fost necesar să introducem și să operăm mai multe routere suplimentare în rețeaua I2P aflată în funcțiune. Aceasta este o practică standard în studiul rețelelor de anonimitate, după cum demonstrează numeroase lucrări anterioare dedicate rețelei Tor. Echipa I2P operează, la rândul său, un router I2P pentru colectarea informațiilor necesare dezvoltării proiectului. În special, site-ul **stats.i2p** furnizează grafice privind performanța rețelei, ajutând dezvoltatorii I2P să monitorizeze funcționarea acesteia și să evalueze eficiența modificărilor introduse în fiecare versiune a software-ului.

Comunitatea I2P a elaborat un set de recomandări pentru desfășurarea responsabilă a cercetărilor în cadrul rețelei, recomandări pe care le-am respectat cu strictețe. În conformitate cu acestea, am menținut un dialog permanent cu echipa I2P privind obiectivele studiului și metodologia noastră de măsurare.

Respectând principiul colectării minimale a datelor, am extras din netDb doar informațiile strict necesare:

- adresa IP a fiecărui nod;
- valoarea hash asociată;
- informațiile privind capacitatea disponibile în obiectele RouterInfo.

După finalizarea analizelor statistice, toate datele colectate au fost șterse în condiții de siguranță. Singurele informații publicate sunt statistici agregate rezultate din aceste date.

S-ar putea argumenta că colectarea temporară a adreselor IP reprezintă o posibilă încălcare a confidențialității utilizatorilor. Problema dacă adresele IP constituie sau nu informații de

identificare personală (*Personally Identifiable Information – PII*) este controversată în numeroase jurisdicții.

Conform secțiunii 3.3.3 din *Guide to Protecting the Confidentiality of Personally Identifiable Information*, publicat de NIST***, adresele IP care nu pot fi asociate cu ușurință unor baze de date sau altor surse capabile să identifice persoane concrete nu sunt considerate informații de identificare personală.*** Din acest motiv, adresele IP observate în cadrul măsurătorilor noastre nu pot fi considerate **informații de identificare personală**, deoarece nu sunt corelate cu alte date colectate în timpul experimentelor care ar putea conduce la identificarea unor persoane.

Trebuie remarcat faptul că arhitectura actuală a I2P nu ascunde utilizarea rețelei față de furnizorul de servicii Internet (ISP) al utilizatorului. Software-ul routerului I2P are rolul de a păstra confidențialitatea mesajelor și anonimatul dintre participanți, nu de a ascunde existența conexiunii la rețea.

Chiar și în aceste condiții, datele legate de adresele IP trebuie analizate responsabil, astfel încât riscul expunerii lor către terți să fie minimizat înainte de ștergere. De exemplu, atunci când asociem adrese IP cu localizări geografice, nu utilizăm API-uri publice. În schimb, folosim o versiune instalată local a bazei de date MaxMind, realizând procesul de geolocalizare complet offline.

În timp ce lucrările anterioare au interogat intensiv serverele *reseed* și routerele ***floodfill*** pentru a colecta informații din *netDb*, noi monitorizăm rețeaua exclusiv în mod pasiv, pentru a evita orice interferență sau încărcare inutilă a altor participanți I2P.

I2P poate fi lansată într-un mod de rețea virtuală pentru studii dedicate testării atacurilor asupra rețelei. Totuși, experimentarea într-un mediu virtual nu răspunde obiectivelor cercetării noastre, care urmărește estimarea populației de participanți I2P și evaluarea rezistenței rețelei la blocare.

Trebuie subliniat faptul că, pe durata întregului studiu, nu doar că am adăugat capacitate suplimentară de rutare rețelei I2P, ci am contribuit și la menținerea bazei de date distribuite a rețelei. Dacă luăm în considerare doar experimentul principal desfășurat pe parcursul a trei luni, fiecare router aflat sub controlul nostru a fost configurat să ofere o lățime de bandă partajată de 8 MB/s în fiecare direcție, cea mai mare valoare observată în exploatare fiind de 5 MB/s.

4. Metodologie

Întrucât I2P este o rețea distribuită, lipsită de orice centralizare, pentru a răspunde întrebărilor noastre de cercetare privind dimensiunea rețelei și rezistența acesteia la cenzură este necesară o abordare de tip *black-box*. În practică, există mai multe modalități prin care un adversar poate colecta informații din baza de date a rețelei I2P (netDb).

De exemplu, acesta poate interoga în mod repetat serverele *reseed* predefinite pentru a obține cât mai multe obiecte RouterInfo. Pentru a limita astfel de activități malițioase, serverele *reseed* sunt concepute să furnizeze același set de RouterInfo atunci când cererile provin de la aceeași sursă. Totuși, un adversar care controlează un număr mare de adrese IP poate continua să colecteze informații din netDb prin interogarea serverelor *reseed* folosind adrese IP diferite.

O altă metodă de extragere a informațiilor din netDb constă în exploatarea agresivă a mecanismului bazei de date prin intermediul interfeței *DatabaseLookupMessag*e (DLM). În mod normal, participanții care nu dețin suficiente obiecte RouterInfo în

copia lor locală a *netDb*, precum și cei care trebuie să localizeze anumite LeaseSet-uri, trimit mesaje DLM către routerele floodfill pentru a solicita informații suplimentare.

Profitând de acest mecanism, un adversar ar putea modifica codul sursă al software-ului routerului I2P astfel încât clienții controlați de el să interogheze în mod repetat routerele *floodfill*, colectând agresiv un număr cât mai mare de obiecte RouterInfo.

În contextul cercetării noastre, metodele descrise mai sus sunt atât impractice, cât și discutabile din punct de vedere etic. Deși unul dintre obiectivele acestei lucrări este estimarea populației participanților I2P, ceea ce presupune colectarea unui număr cât mai mare de obiecte RouterInfo din netDb, considerăm că acest proces trebuie realizat într-o manieră responsabilă.

Principiul pe care l-am urmat este că experimentele nu trebuie să genereze trafic inutil și nici să consume excesiv resursele altor participanți I2P din rețea. Liu și colaboratorii au arătat că interogarea repetată a serverelor *reseed* contribuie cu doar 7,04% la numărul total de participanți identificați, în timp ce manipularea mecanismului netDb contribuie cu doar 30,18%.

Din acest motiv, am ales o metodă alternativă și am desfășurat experimentele într-o manieră pasivă, prin operarea mai multor routere care doar observă activitatea rețelei.

Obiectivul principal al experimentelor noastre *este să determinăm de câte routere I2P este nevoie și în ce condiții trebuie configurate acestea pentru a monitoriza eficient o parte semnificativă a rețelei I2P cu un efort minim*.

Pentru a evita limitările privind lățimea de bandă întâlnite în cercetările anterioare, toate experimentele noastre au fost realizate

pe servere private dedicate, nu pe infrastructuri de cercetare partajate cu alți cercetători.

4.1. Specificațiile sistemelor utilizzate

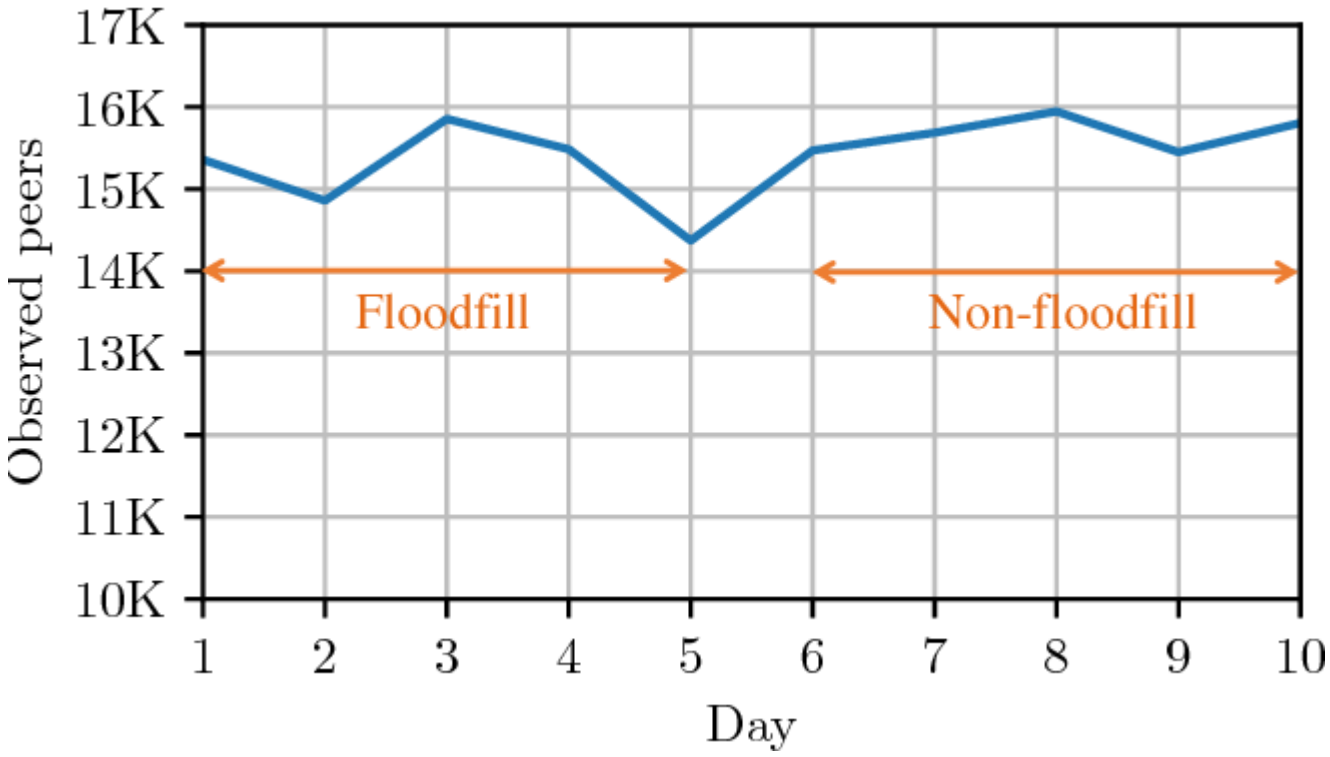

Figura 2. Numărul de participanți observați în cadrul experimentului inițial, realizat pentru evaluarea impactului diferitelor configurații hardware și software.

Întrucât nu există recomandări oficiale privind operarea unui router I2P de înaltă performanță, am adoptat o abordare pragmatică pentru a determina ce specificații sunt suficiente pentru a observa un număr semnificativ de alte routere I2P. Parametrii analizați includ atât configurația hardware a sistemului gazdă (de exemplu procesorul și memoria RAM), cât și parametrii de configurare ai software-ului routerului I2P (de exemplu lățimea de

bandă partajată, numărul maxim de tuneluri la care poate participa și dimensiunea memoriei heap alocate mașinii virtuale Java).

Trebuie precizat că implementarea oficială a routerului I2P este scrisă în Java. Înțelegerea comportamentului acestui software reprezintă o etapă necesară a studiului nostru. De exemplu, creșterea numărului de conexiuni acceptate de un router fără ajustarea corespunzătoare a memoriei *heap* disponibile pentru Java poate genera erori care obligă routerul să se repornească. În mod similar, dacă resursele procesorului sunt insuficiente, routerul poate pierde conexiuni, poate introduce blocaje sau poate crește latența.

Toate aceste situații sunt penalizate de algoritmul de clasificare utilizat de I2P, ceea ce reduce probabilitatea ca routerul respectiv să fie selectat pentru construirea tunelurilor altor participanți. În consecință, un router configurat necorespunzător va avea o vizibilitate mai redusă asupra rețelei decât unul capabil să mențină un nivel ridicat al calității serviciului.

Am investigat empiric limitele superioare ale resurselor necesare pentru a determina configurația optimă a sistemelor folosite în experimente.

În mod intuitiv, știm că un router mai performant va observa un număr mai mare de obiecte RouterInfo. Ca punct de plecare, am rulat un router I2P pe un sistem performant dotat cu:

- procesor cu 10 nuclee la 2,40 GHz;
- 16 GB memorie RAM.

Lățimea de bandă partajată a acestui router a fost configurată la 8 MB/s, deoarece filtrul Bloom integrat în software-ul routerului

I2P este limitat la această valoare. Numărul maxim de tuneluri la care routerul putea participa a fost stabilit la 15.000, iar pentru memoria heap a mașinii virtuale Java au fost alocați 10 GB.

După funcționarea routerului timp de zece zile, câte cinci zile în fiecare mod de operare (floodfill și non-floodfill), am făcut următoarele observații:

- Utilizarea totală a procesorului s-a menținut constant în intervalul 4-5 GHz.
- Consumul de memorie s-a situat, în cea mai mare parte a timpului, între 3 și 4 GB.
- Cea mai mare lățime de bandă observată a fost de 5 MB/s.
- Numărul de tuneluri la care routerul participa a rămas în jurul valorii de 4.000, iar valoarea maximă observată a fost de aproximativ 5.500 de tuneluri.
- Toate valorile maxime menționate mai sus au fost observate în modul non-floodfill.

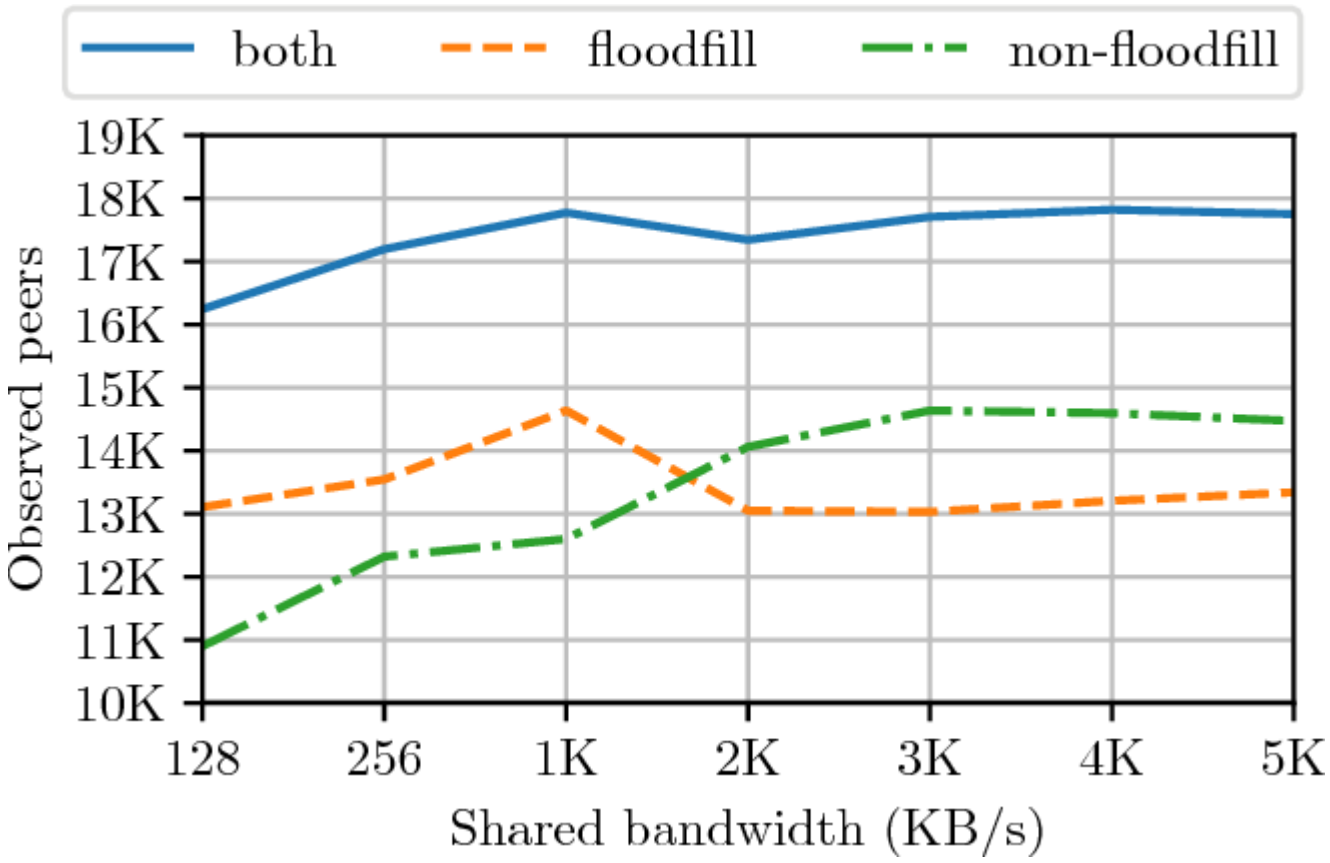

Figura 3. Numărul de participanți I2P observați prin operarea a 14 noduri
(7 în mod *floodfill* și 7 în mod *non-floodfill*) cu lățime de bandă partajată crescută progresiv.

Conform Figurii 2, deși numărul de participanți observați în modul *non-floodfill* este ușor mai mare decât în modul *floodfill*, acesta rămâne constant în jurul valorii de 15.000-16.000 de participanți. Trebuie reținut că un participant este identificat printr-o valoare hash unică inclusă în obiectul său RouterInfo.

Pe baza acestor observații, am configurat mașinile (virtuale) utilizate în experimentele ulterioare cu următoarele specificații maxime:

- 3 nuclee CPU la 2,4 GHz, însumând 7,2 GHz;
- 5 GB RAM, dintre care:

- 4 GB alocați memoriei heap a mașinii virtuale Java;
- 1 GB rezervat restului sistemului;

- numărul maxim de tuneluri participante setat la 10.000;
- lățimea de bandă partajată maximă setată la 8 MB/s, corespunzător limitei impuse de filtrul Bloom integrat în software-ul routerului I2P.

4.2. Operarea în mod Floodfill versus Non-floodfill

Deși Figura 2 arată că numărul de participanți observați în modul non-floodfill este ușor mai mare decât în modul floodfill, este posibil ca această diferență să fie rezultatul unor fluctuații ale numărului de participanți activi zilnic în perioada studiului. Din acest motiv, am operat simultan alte 14 routere, atât în mod floodfill, cât și în mod non-floodfill, pentru a elimina influența eventualelor variații ale populației zilnice asupra observațiilor noastre.

Cele 14 routere au fost împărțite în două grupuri:

- 7 routere *non-floodfill*;
- 7 routere *floodfill*.

Pentru fiecare grup, am crescut treptat lățimea de bandă partajată după următoarele valori:

- 128 KB/s;
- 256 KB/s;
- 1 MB/s;
- 2 MB/s;

- 3 MB/s;
- 4 MB/s;
- 5 MB/s.

Am ales valoarea de 128 KB/s ca limită inferioară deoarece reprezintă pragul minim necesar pentru ca un router să poată primi marcajul *floodfill*. Valoarea maximă a fost stabilită pe baza celui mai mare consum de lățime de bandă observat în experimentul anterior (Secțiunea 4.1). Aceste routere au fost rulate pe sisteme cu specificațiile hardware descrise anterior.

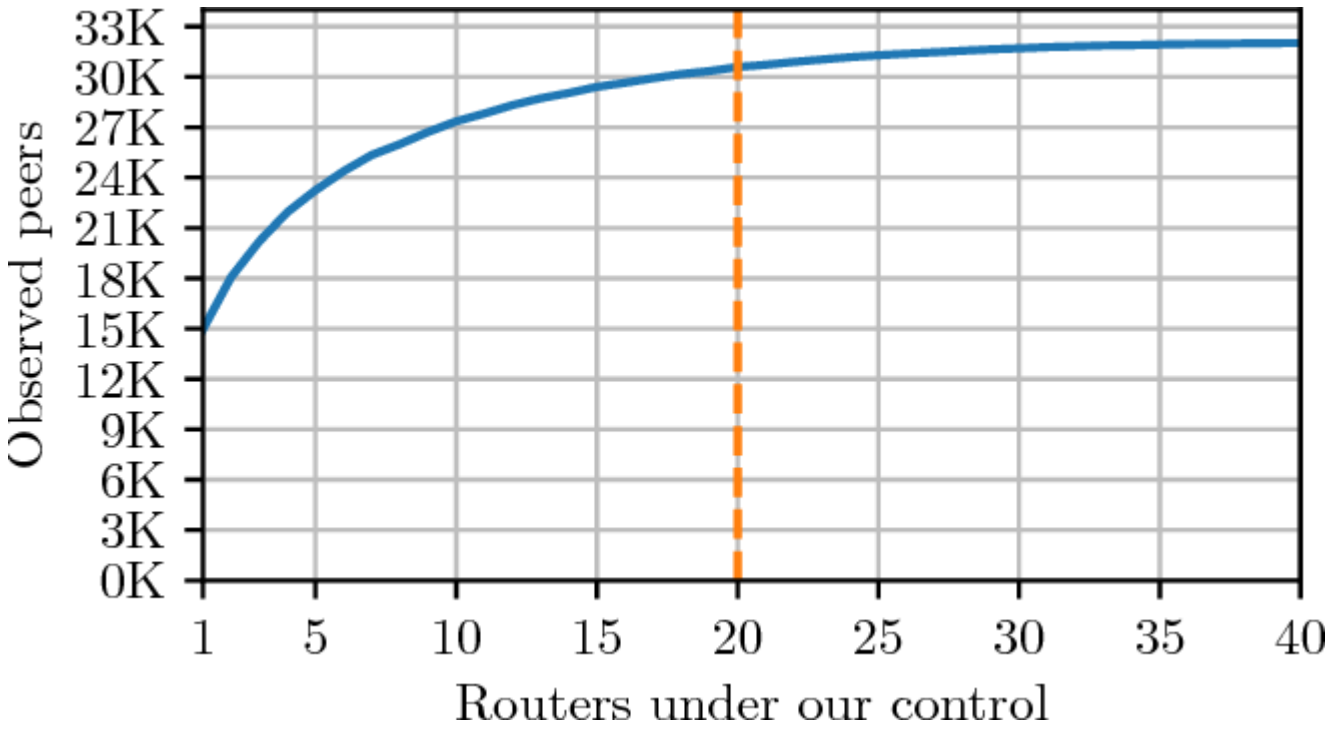

Figura 4. Numărul cumulativ de participanți observați prin operarea a 1 până la 40 de routere.

Figura 3 arată că routerele floodfill cu lățime de bandă partajată sub 2 MB/s observă cu aproximativ 1.500-2.000 de participanți mai

mult decât routerele non-floodfill configurate cu aceeași lățime de bandă.

Pe de altă parte, routerele non-floodfill cu lățime de bandă partajată mai mare de 2 MB/s observă cu aproximativ 1.000-1.500 de participanți mai mult decât routerele floodfill cu aceeași lățime de bandă.

Există însă o observație interesantă: atunci când sunt combinate datele provenite de la fiecare pereche de routere care utilizează aceeași lățime de bandă, numărul total de participanți observați (linia superioară din grafic) rămâne în jurul valorii de 17.000-18.000, indiferent de diferențele de lățime de bandă și de variațiile dintre modurile de operare.

Pentru a explica acest comportament, am identificat patru modalități principale prin care participanții I2P află informații despre alți participanți ai rețelei:

- În cadrul procesului de inițializare (*bootstrapping*), un participant nou conectat descarcă obiecte RouterInfo de la un set de servere *reseed* predefinite pentru a obține o imagine parțială a rețelei. Conform jurnalelor furnizate de consola routerului I2P, un participant nou descarcă aproximativ 150 RouterInfo de la două servere *reseed* (aproximativ 75 de la fiecare server).

- Un router care nu dispune de suficiente obiecte RouterInfo în stocarea locală trimite un mesaj DatabaseLookupMessage (DLM) către routerele *floodfill* pentru a solicita informații suplimentare.

- Un router activ poate fi selectat de alți participanți pentru a ruta trafic în numele lor. În acest fel, routerul află informații

despre alte routere aflate în vecinătatea tunelurilor la care participă. Cu cât specificațiile unui router sunt mai bune, cu atât probabilitatea de a fi selectat pentru un număr mai mare de tuneluri este mai ridicată.

- Un router floodfill primește obiecte RouterInfo publicate de alte routere non-floodfill aflate „în apropiere” sau de alte routere floodfill, prin intermediul mecanismului de propagare (*flooding*). Distanța de „proximitate” este calculată pe baza distanței XOR dintre cheile de indexare ale celor două routere. Mecanismul de *flooding* este activat atunci când un router *floodfill* primește un mesaj DatabaseStoreMessage care conține un obiect RouterInfo sau LeaseSet valid și mai recent decât versiunea stocată local în netDb. În această situație, routerul transmite mai departe informația către trei dintre cele mai apropiate routere *floodfill*.

Considerăm că diferențele observate sunt generate în principal de ultimele două mecanisme descrise mai sus, deoarece acestea reprezintă principalele modalități prin care routerele noastre descoperă alți participanți ai rețelei.

Cele două grupuri de routere interacționează cu rețeaua în moduri diferite, ceea ce înseamnă că fiecare grup obține o perspectivă proprie asupra rețelei, inaccesibilă celuilalt grup. Din acest motiv, agregarea datelor colectate de ambele grupuri oferă o imagine mai completă asupra rețelei în ansamblu.

Pe scurt, acest experiment ne arată că este important să operăm simultan routere atât în modul non-floodfill, cât și în modul floodfill. Combinarea acestor perspective complementare permite obținerea unei imagini mult mai complete asupra rețelei I2P.

4.3. Numărul de routere

În continuare, am investigat câte routere trebuie să operăm pentru a observa o parte semnificativă a rețelei. Înaintea acestei lucrări, Liu și colaboratorii au utilizat diverse metode pentru colectarea informațiilor din netDb: interogarea repetată a serverelor *reseed*, trimiterea continuă de mesaje DLM către alte routere *floodfill* și operarea simultană a unor routere *floodfill* și *non-floodfill*. Autorii au susținut că au descoperit 94,9% dintre toate routerele din rețea, comparând datele colectate cu statisticile publicate pe site-ul stats.i2p.

Totuși, după discuțiile purtate cu echipa I2P, am confirmat că aceste statistici nu pot fi considerate o referință absolută. Motivul este că datele sunt colectate doar de la un router obișnuit de tip *non-floodfill* și nu de la un router cu lățime mare de bandă. În plus, rezultatele raportate sunt construite pe baza datelor agregate pe ultimele treizeci de zile și nu reflectă situația zilnică a rețelei.

Mai recent, Gao și colaboratorii au operat 40 de routere *floodfill* pentru colectarea de LeaseSet-uri și au afirmat că au identificat peste 80% dintre toate eepsite-urile ascunse. Totuși, nu este clar ce combinație de hardware și software a fost utilizată pentru operarea acestor routere. Mai important, obiectivul nostru este colectarea de RouterInfo-uri, nu de LeaseSet-uri. Din acest motiv, operarea tuturor routerelor într-un singur mod de funcționare (*floodfill* sau *non-floodfill*) nu este o soluție optimă, după cum am discutat în Secțiunea 4.2.

Din această cauză, am ales să operăm un total de 40 de routere, împărțite în mod egal între cele două moduri de funcționare:

- 20 de routere *floodfill*;
- 20 de routere *non-floodfill*.

Fiecare router a fost găzduit pe un sistem cu specificațiile prezentate în Secțiunea 4.1.

Întrucât obiectele RouterInfo sunt salvate pe disc prin design, astfel încât să rămână disponibile după repornirea routerului, am monitorizat directorul netDb în care acestea sunt stocate.

Trebuie menționat că, deși structura de date RouterInfo conține un câmp de expirare, acesta nu este utilizat în implementarea actuală. Din această cauză, durata reală de activitate a unui participant nu poate fi determinată direct. Cu alte cuvinte, existența unui anumit obiect RouterInfo confirmă doar prezența participantului în rețea la un moment dat, fără a indica intervalul exact în care acesta a rămas activ.

Deoarece routerele floodfill aplică un termen de expirare de o oră pentru toate obiectele RouterInfo stocate local, am ales să monitorizăm directorul netDb la intervale de o oră pentru a surprinde fiecare nou obiect RouterInfo apărut.

La fiecare 24 de ore:

- curățam directorul netDb;
- eliminam toate înregistrările existente;
- evitam astfel numărarea participanților inactivi în ziua următoare.

După operarea celor 40 de routere timp de cinci zile, am calculat numărul cumulativ de participanți observați zilnic de întregul grup de routere.

Figura 4 arată că operarea a 40 de routere ne permite să observăm aproximativ 32.000 de participanți în rețea.

Relația dintre numărul de participanți observați și numărul de routere aflate sub controlul nostru urmează o curbă logaritmică. Graficul arată că numărul participanților observați crește rapid atunci când numărul routerelor este mărit de la 1 la 20, după care creșterea încetinește și converge către aproximativ 32.000 de participanți.

Mai exact, folosirea a 20 de routere ne permite deja să observăm 95,5% din totalul participanților identificați, adică peste 30.500 de participanți.

După pragul de 35 de routere, fiecare router suplimentar contribuie la identificarea a doar 10-30 de participanți în plus.

Pe baza acestor rezultate, concluzionăm că 20 de routere sunt suficiente pentru a obține o imagine foarte bună asupra rețelei I2P.

5. Măsurarea rețelei

Ținând cont de observațiile prezentate în Secțiunea 4, am realizat măsurătorile prin operarea a **20 de routere**, folosind specificațiile hardware definite în Secțiunea 4.1.

Acest grup a fost alcătuit din:

- **10 routere floodfill**;
- **10 routere non-floodfill**.

Am colectat obiectele **RouterInfo** observate de aceste routere pe o perioadă de **trei luni**, din februarie până în aprilie 2018.

5.1. Populația participanților I2P

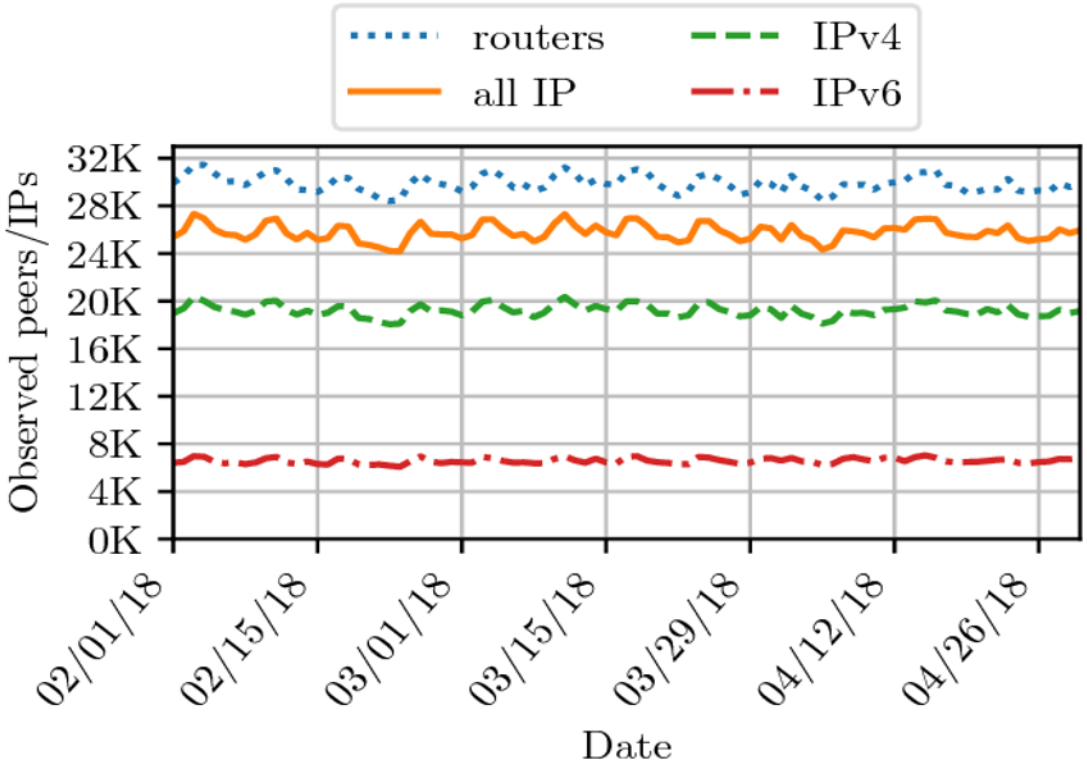

Figura 5. Numărul de participanți unici și de adrese IP unice.

Figura 5 prezintă numărul de participanți I2P unici și de adrese IP unice, incluzând atât IPv4, cât și IPv6, observate pe parcursul perioadei de trei luni. Numărul participanților activi zilnic se menține relativ stabil, în jurul valorii de 30.500.

Trebuie remarcat că un participant I2P este identificat printr-un identificator criptografic, reprezentat de o valoare *hash* unică inclusă în obiectul său RouterInfo. Acest identificator este generat la prima instalare a software-ului routerului I2P și rămâne neschimbat pe întreaga durată de viață a participantului.

În ceea ce privește numărul adreselor IP unice, am contabilizat zilnic toate adresele IPv4 și IPv6 distincte asociate routerelor I2P care oferă suport pentru aceste protocoale. Având în vedere că unii participanți își schimbă frecvent adresele IP, după cum vom discuta

în Secțiunea 5.2.2, ne-am fi așteptat ca numărul total de adrese IP unice să fie mai mare decât numărul participanților.

Totuși, după cum arată Figura 5, numărul total de adrese IP este semnificativ mai mic decât numărul participanților.

Analizând obiectele RouterInfo colectate, am identificat un număr mare de participanți I2P ale căror fișiere RouterInfo nu conțin o adresă IP validă. Cu alte cuvinte, adresele IP publice ale acestor participanți sunt necunoscute.

Am examinat apoi și celelalte câmpuri din obiectele RouterInfo ale acestor participanți și am descoperit că grupul participanților fără adresă IP cunoscută poate fi împărțit în două subgrupuri:

- participanți *firewalled*;
- participanți *hidden*.

Participanții *firewalled* funcționează în spatele unor dispozitive NAT sau al unor configurații restrictive de firewall.

Participanții *hidden* folosesc alți participanți pentru a-și ruta traficul, dar nu contribuie la rutarea traficului altor participanți, deoarece nu își publică adresa IP în baza de date a rețelei.

În mod implicit, participanții aflați în țări cu scoruri reduse privind libertatea presei (adică scoruri mai mari de 50) sunt configurați în modul *hidden*. Totuși, această setare poate fi modificată pentru a permite expunerea participantului către restul rețelei, ceea ce poate conduce la o integrare mai bună și, implicit, la performanțe superioare.

Am clasificat aceste două categorii analizând câmpul adreselor IP asociate nodurilor de introducere (*introducers*) din fiecare fișier RouterInfo.

I2P oferă o metodă prin care participanții aflați în spatele unor dispozitive NAT sau firewall-uri pot comunica cu restul rețelei folosind puncte de introducere operate de terți, numite introducers.

De exemplu, un participant I2P, precum Bob, aflat în spatele unui firewall care blochează pachetele de intrare nesolicitate, poate selecta mai mulți participanți ai rețelei pentru a acționa ca *introducers*. Fiecare dintre aceștia generează un identificator de introducere pentru Bob. Aceste identificatoare sunt apoi publicate și utilizate de alți participanți pentru a iniția comunicarea cu el.

Dacă Alice dorește să comunice cu Bob, ea trimite o cerere către unul dintre *introducers*, solicitând să fie pusă în legătură cu Bob. Nodul de introducere transmite apoi cererea către Bob, incluzând adresa IP publică și portul folosit de Alice, și trimite simultan un răspuns către Alice care conține adresa IP publică și portul lui Bob.

După ce primește informațiile despre Alice, Bob trimite un mic pachet de date către adresa și portul acesteia, realizând astfel o perforare a firewall-ului (*hole punching*), ceea ce permite stabilirea comunicației directe.

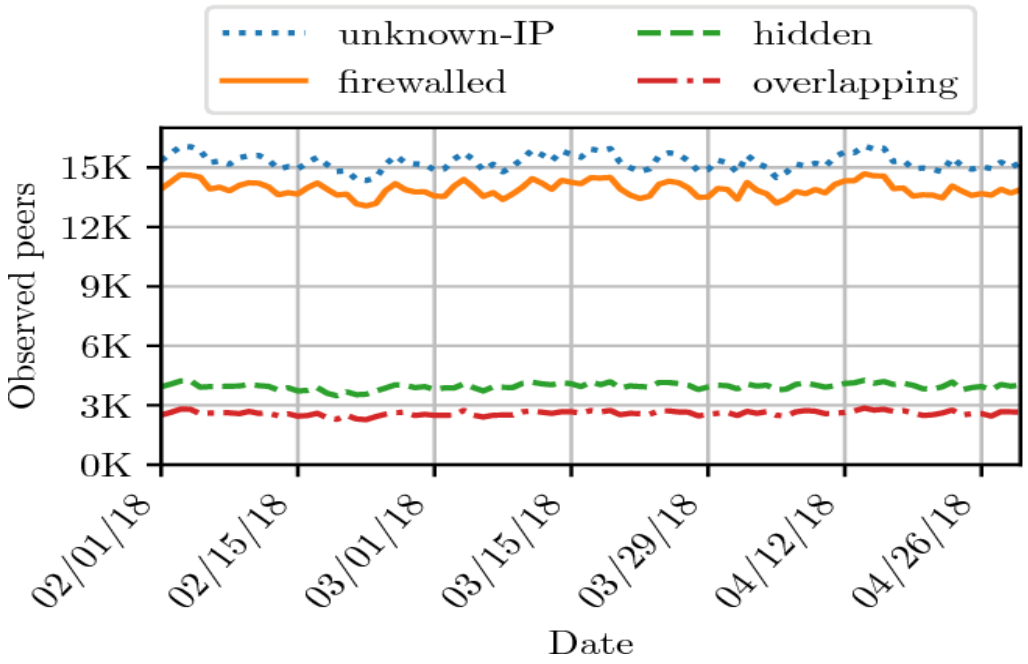

Figura 6. Numărul participanților cu adrese IP necunoscute.

Prin examinarea câmpurilor referitoare la punctele de introducere din obiectele RouterInfo, putem diferenția participanții *firewalled* de cei *hidden*.

Un participant *firewalled* conține în obiectul său RouterInfo informații despre *introducers*, în timp ce un participant *hidden* nu conține astfel de informații.

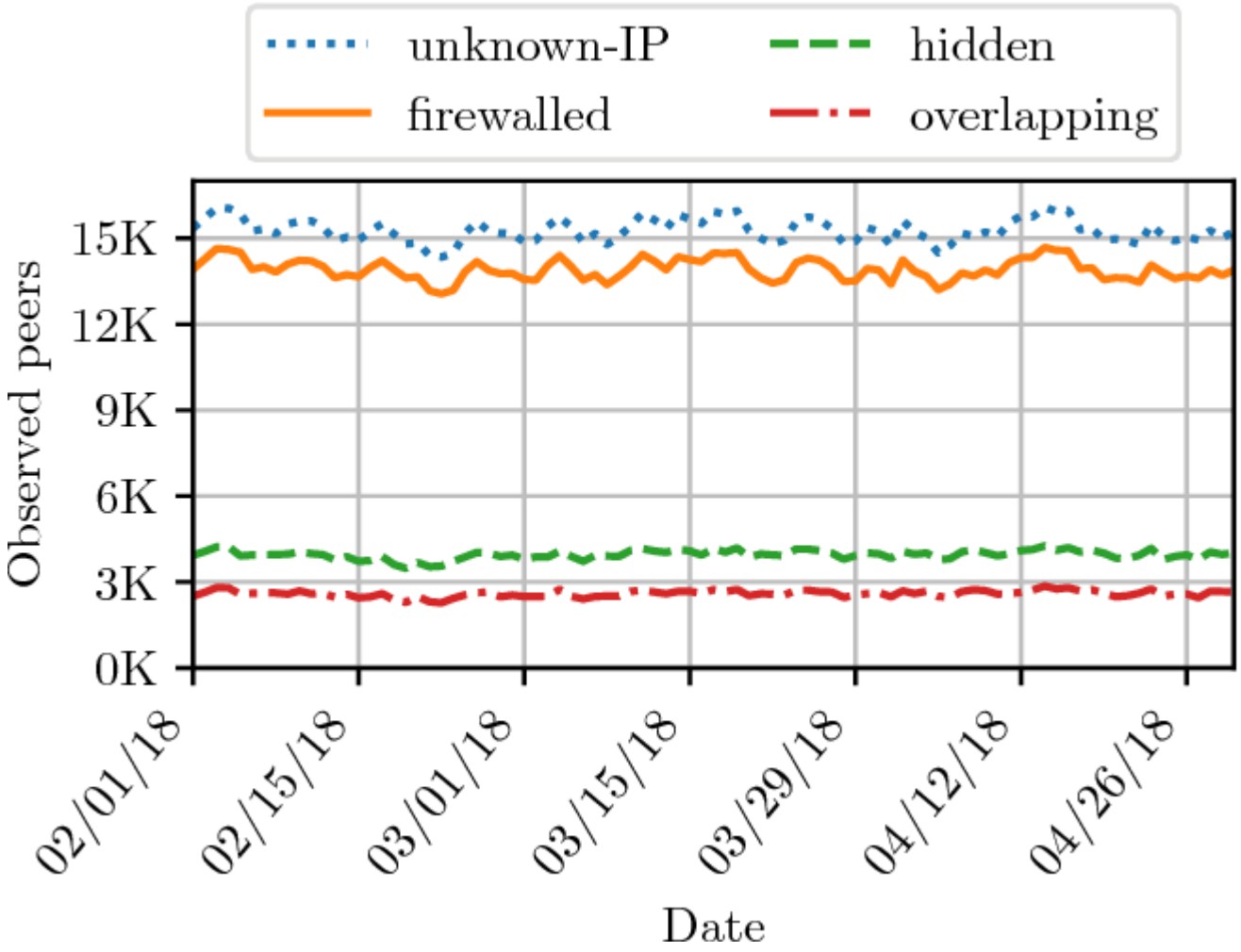

Figura 6 arată distribuția participanților între aceste două categorii.

În total, există peste 15.000 de participanți pe zi cu adrese IP necunoscute, dintre care:

- aproximativ 14.000 sunt participanți *firewalled*;
- aproximativ 4.000 sunt participanți *hidden*.

Între aceste două grupuri există o suprapunere de aproximativ 2.600 de participanți. Cu alte cuvinte, în fiecare zi aproximativ 2.600 de participanți I2P își schimbă statutul între *firewalled* și *hidden*.

5.2. Rata de fluctuație a nodurilor (*Churn Rate*)

I2P este o rețea P2P dinamică, în care participanții se conectează și se deconectează frecvent. Înaintea acestei lucrări, Timpanaro și colaboratorii au realizat primul studiu privind rata de fluctuație a participanților în I2P și au raportat că probabilitatea ca un participant I2P să devină offline după 30 de minute este de aproximativ 15%. Totuși, experimentul lor a fost desfășurat pe o perioadă de doar cinci zile și a implicat numai opt routere *floodfill*.

Liu și colaboratorii au desfășurat un experiment pe durata a aproximativ două săptămâni și au raportat că 19,03% dintre participanții observați au rămas activi timp de o zi, iar 48,66% au rămas activi mai mult de șapte zile.

În ansamblu, aceste cercetări au fost efectuate pe perioade scurte și la o scară redusă, oferind o imagine incompletă asupra ratei de fluctuație din rețeaua I2P. În plus, niciunul dintre studiile anterioare nu a analizat fenomenul schimbării adreselor IP ale participanților, fenomen frecvent întâlnit deoarece majoritatea furnizorilor de servicii Internet nu alocă adrese IP statice conexiunilor rezidențiale.

În această secțiune analizăm obiectele RouterInfo colectate pentru a acoperi aceste lacune de cercetare.

5.2.1. Longevitatea participanților

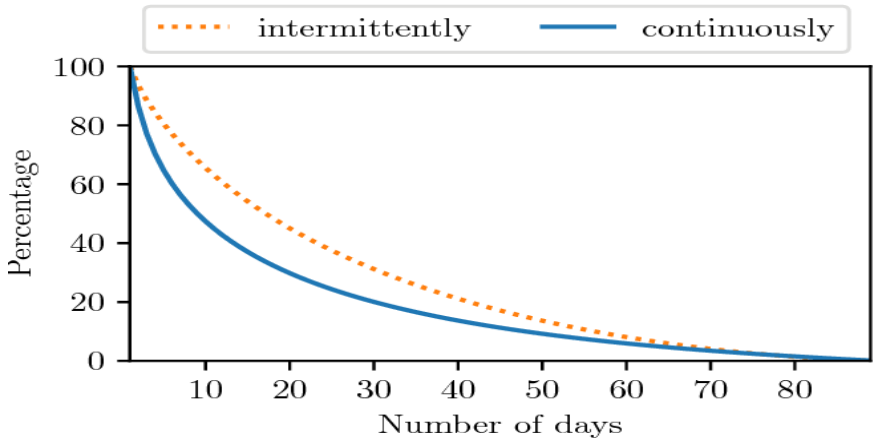

Figura 7. Procentul participanților observați în rețea continuu sau intermitent timp de *n* zile.

Figura 7 prezintă rata de fluctuație a participanților I2P pe parcursul perioadei noastre de măsurare de trei luni.

După cum se observă în Figura 7, procentele participanților care rămân în rețea mai mult de șapte zile sunt:

- 56,36% în mod continuu;
- 73,93% în mod intermitent.

Pentru participanții care rămân online mai mult de 30 de zile, procentele sunt:

- 20,03% în mod continuu;
- 31,15% în mod intermitent.

Deși I2P este o rețea P2P complet distribuită și foarte dinamică, aceste rezultate indică faptul că mai mult de jumătate dintre participanți rămân stabili în rețea timp de peste o săptămână.

Comparativ cu rata de 48,66% raportată în 2014 de Liu și colaboratorii, valorile obținute de noi, atât pentru prezența continuă, cât și pentru cea intermitentă, sugerează că rețeaua a devenit mai stabilă în timp.

5.2.2. Fluctuația adreselor IP

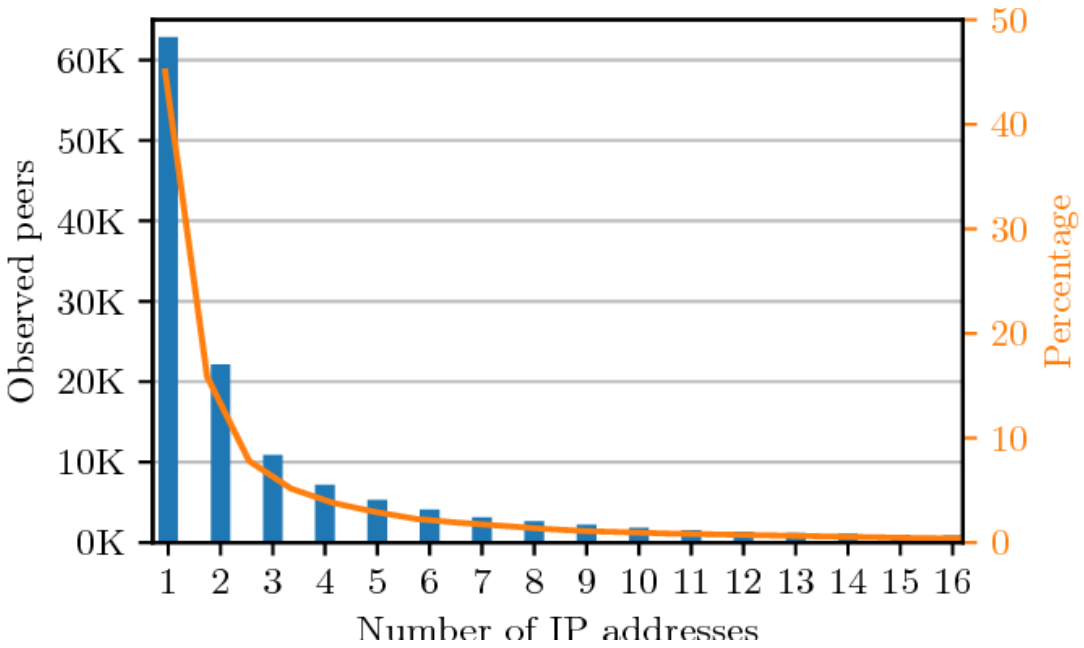

Figura 8. Numărul de adrese IP asociate participanților I2P.

Deoarece majoritatea furnizorilor de servicii Internet nu alocă adrese IP statice conexiunilor rezidențiale, este normal ca un participant să fie asociat cu mai multe adrese IP de-a lungul timpului.

După cum arată Figura 8, există aproximativ:

- 63.000 de participanți asociați cu o singură adresă IP, reprezentând 45% dintre participanții cu adresă IP cunoscută;
- peste 76.000 de participanți asociați cu cel puțin două adrese IP, reprezentând 55% dintre participanții cu adresă IP cunoscută.

Am observat, de asemenea, un grup restrâns de aproximativ 460 de participanți care au fost asociați cu peste o sută de adrese IP diferite pe parcursul celor trei luni de studiu. Aceștia reprezintă

aproximativ 0,65% din totalul participanților cu adresă IP cunoscută.

Vom analiza mai detaliat acest fenomen în Secțiunea 5.3.2, dedicată distribuției geografice a participanților I2P.

5.3. Distribuția participanților

Participanții din rețeaua I2P sunt clasificați prin diverse indicatori de capacitate (*capacity flags*), stabiliți în funcție de:

1. modul de operare (*floodfill* sau *non-floodfill*);
2. accesibilitate (dacă pot fi contactați sau nu de alți participanți);
3. lățimea de bandă partajată.

Acești indicatori sunt reprezentați prin câte o singură literă majusculă și sunt stocați în fișierul RouterInfo al fiecărui participant.

Suntem interesați să înțelegem distribuția diferitelor tipuri de participanți în cadrul rețelei I2P.

Înaintea acestui studiu, Liu și colaboratorii au analizat distribuția participanților I2P pe țări. Totuși, existența participanților asociați cu mai multe adrese IP impune o abordare mai riguroasă pentru analiza celor care își schimbă frecvent adresa.

Așa cum am menționat în Secțiunea 5.2.2, mai mult de jumătate dintre participanții cu adresă IP cunoscută sunt asociați cu două sau mai multe adrese IP.

În această secțiune analizăm două aspecte principale ale participanților I2P:

- distribuția capacității;
- distribuția geografică.

Provide your feedback on BizChat

5.3.1. Distribuția capacității participanților

Indicatorii de capacitate (*capacity flags*) sunt utilizați de participanții din rețea pentru luarea unor decizii fundamentale, precum selectarea nodurilor pentru construirea tunelurilor sau alegerea routerelor floodfill către care sunt trimise informațiile RouterInfo și LeaseSet.

Statutul unui participant este definit astfel:

- Un router **floodfill** este marcat prin indicatorul **f** în câmpul de capacitate, în timp ce un router **non-floodfill** nu conține acest indicator.
- Intervalul estimat al lățimii de bandă partajate este indicat prin una dintre cele șapte litere disponibile: K, L, M, N, O, P și X, care corespund următoarelor valori:
  - K: sub 12 KB/s
  - L: 12-48 KB/s
  - M: 48-64 KB/s
  - N: 64-128 KB/s
  - O: 128-256 KB/s
  - P: 256-2000 KB/s
  - X: peste 2000 KB/s

- Accesibilitatea unui participant este indicată prin:
  - R (*reachable*) – accesibil;
  - U (*unreachable*) – inaccesibil.

De exemplu, indicatorii OfR din câmpul de capacitate al unui participant arată că acesta este:

- un router **floodfill**;
- accesibil altor participanți;
- cu o lățime de bandă partajată între 128 și 256 KB/s.

Analiza acestor indicatori oferă o imagine mai clară asupra distribuției capacităților participanților și permite estimarea mai precisă a populației totale a rețelei.

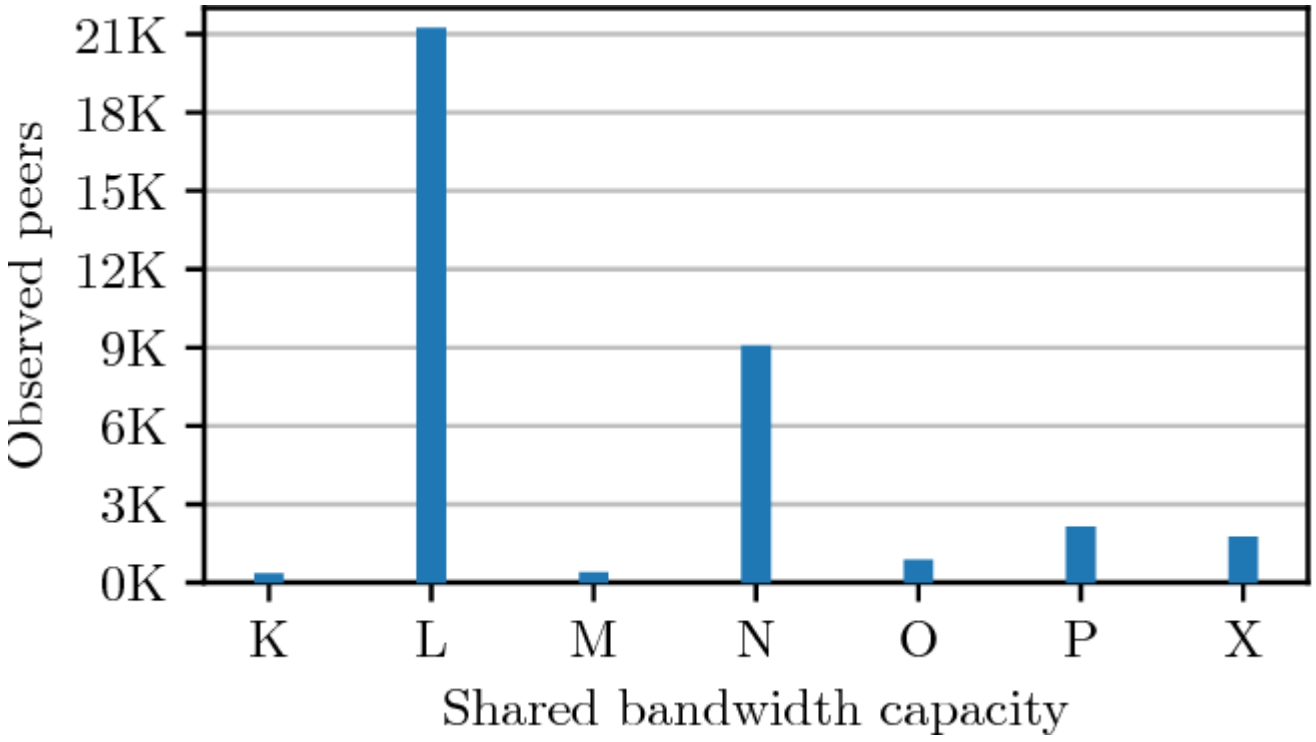

Figura 9. Distribuția capacităților participanților I2P.

Analiza prezentată în Figura 9 arată că participanții marcați cu indicatorul L sunt cei mai numeroși din rețea, cu o medie de aproximativ 21.000 de participanți pe zi. Acest rezultat este în concordanță cu faptul că indicatorul L reprezintă configurația implicită de lățime de bandă a software-ului routerului I2P.

Cu peste 9.000 de participanți pe zi, categoria N ocupă locul al doilea.

Celelalte categorii au următoarele valori medii zilnice:

- P: aproximativ 2.100 participanți;
- X: aproximativ 1.800 participanți;
- O: aproximativ 875 participanți;
- M: aproximativ 400 participanți;
- K: aproximativ 360 participanți.

În ceea ce privește modul de operare, am observat în medie aproximativ 2.700 de participanți **floodfill** pe zi, reprezentând 8,8% din totalul participanților observați.

Referitor la accesibilitate, numărul participanților accesibili și inaccesibili este aproape identic în majoritatea timpului, situându-se între 15.000 și 16.000 pentru fiecare categorie. Cu alte cuvinte, cele două categorii reprezintă aproximativ câte jumătate din rețea.

Trebuie precizat că participanții inaccesibili includ și participanții cu adresă IP necunoscută descriși în Secțiunea 5.1.

Am analizat în continuare distribuția capacității pentru fiecare dintre cele trei grupuri:

- routere floodfill;

- participanți accesibili;
- participanți inaccesibili.

După cum se observă în Tabelul 1, grupurile accesibil și inaccesibil au o distribuție similară cu cea a întregii rețele: categoria L este dominantă, urmată de categoria N. În schimb, în grupul floodfill, categoria N este cea mai răspândită, iar categoria L ocupă locul al doilea.

Trebuie remarcat faptul că suma tuturor indicatorilor nu este egală cu 100% din două motive:

1. Fluctuațiile lățimii de bandă pot schimba frecvent indicatorul de capacitate al unui participant.
2. Pentru compatibilitate cu versiunile mai vechi ale software-ului I2P, un participant poate publica simultan mai mult de un indicator de lățime de bandă.

Mai exact, indicatorii P și X au fost introduși începând cu versiunea 0.9.20 și înlocuiesc vechiul indicator de capacitate maximă, O. Pentru a asigura compatibilitatea cu versiunile anterioare, un participant marcat cu P sau X păstrează și indicatorul O în câmpul său de capacitate.

Lățime de bandă	Indicator	Floodfill	Accesibil	Inaccesibil	Total
< 12 KB/s	K	0,10	1,14	1,27	1,18

12-48 KB/s	L	26,82	66,62	75,81	69,67
48-64 KB/s	M	2,16	1,44	1,24	1,31
64-128 KB/s	N	62,06	36,79	26,08	29,74
128-256 KB/s	O	5,18	3,15	2,88	2,87
256-2000 KB/s	P	15,97	7,72	6,64	7,05
> 2000 KB/s	X	13,76	6,44	5,49	5,76

Tabelul 1. Procentul routerelor în funcție de lățimea de bandă și statut

În cadrul grupului floodfill, procentul cumulat al participanților marcați cu P și X este de aproximativ 30%, depășind proporția participanților marcați cu L. Acest rezultat este firesc, deoarece modul floodfill este activat automat doar pentru participanții configurați cu limite ridicate de lățime de bandă.

În configurația actuală, cerința minimă pentru un router floodfill este o lățime de bandă partajată de 128 KB/s. Conform regulilor actuale de activare automată, un participant trebuie să dețină cel puțin indicatorul N pentru a deveni automat router floodfill.

Totuși, Tabelul 1 arată că există un grup de routere floodfill cu lățime de bandă mai mică decât pragul minim necesar. Acest grup include participanții marcați cu:

- K;
- L;
- M.

Împreună, aceștia reprezintă aproximativ 30% dintre toate routerele floodfill observate.

Această contradicție se explică prin faptul că operatorii pot forța activarea modului floodfill prin intermediul consolei routerului, indiferent de capacitatea reală a acestuia.

În consecință, routerele floodfill cu adevărat eligibile sunt doar cele marcate cu:

- N;
- O;
- P;
- X,

adică routerele care dispun de suficientă lățime de bandă pentru a deservi eficient mecanismul netDb.

Pornind de la această observație, am considerat routerele floodfill marcate cu K, L și M ca fiind activate manual și neeligibile din punct de vedere al capacității. Am recalculat numărul routerelor floodfill eligibile prin reunirea seturilor N, O, P și X și eliminarea tuturor suprapunerilor cu seturile K, L și M.

Rezultatul arată că 71% dintre routerele floodfill observate sunt exclusiv de tip N, O, P sau X.

Chiar și în interiorul acestui grup există routere performante activate manual, asemenea celor operate de noi. Prin urmare, numărul routerelor floodfill activate automat după îndeplinirea tuturor criteriilor de „sănătate” trebuie să fie mai mic de 1.917, valoare care corespunde estimării publicate pe site-ul oficial I2P în aprilie 2018, unde erau raportate aproximativ 1.700 de routere floodfill.

Conform observațiilor independente ale dezvoltatorilor I2P, aproximativ 6% dintre participanții rețelei sunt routere *floodfill*, și nu 8,8% cum rezultă din observațiile brute prezentate anterior.

Demonstrăm că această diferență este cauzată de existența routerelor *floodfill* activate manual, care nu îndeplinesc efectiv cerințele minime de lățime de bandă.

Pornind de la proporția de 6% a routerelor floodfill activate automat, estimarea rezultată pentru populația totală a rețelei confirmă observațiile din Secțiunea 4.3, conform cărora operarea a 40 de routere permite observarea a aproximativ 32.000 de participanți.

Putem concluziona cu un grad ridicat de încredere că operarea a 20 de routere permite monitorizarea a peste 95,5% din rețeaua I2P.

5.3.2. Distribuția geografică

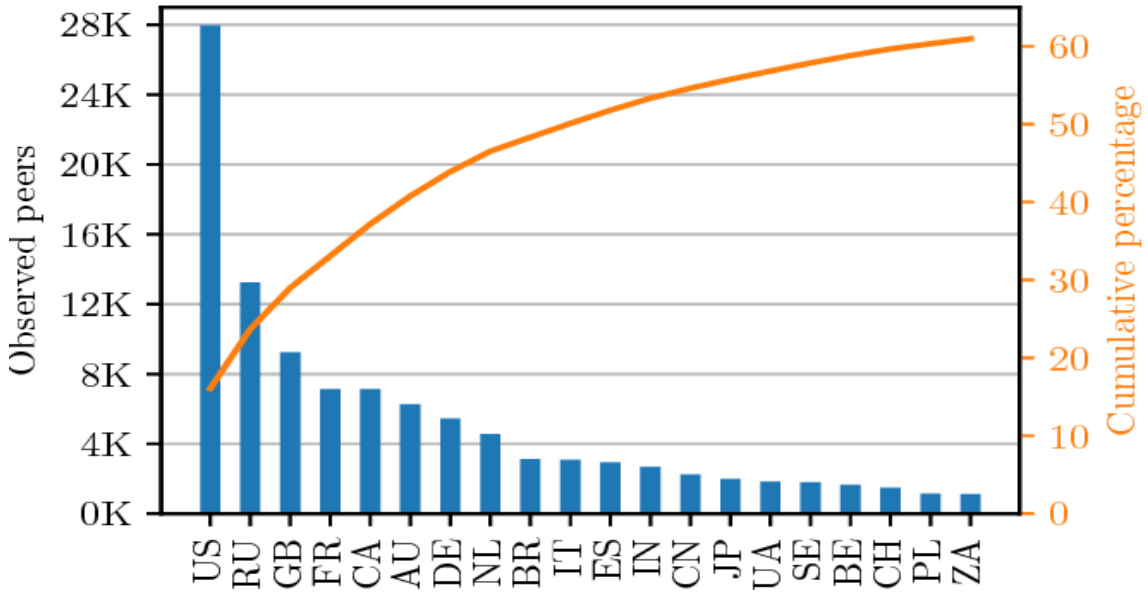

Figura 10. Primele 20 de țări în care se află participanții I2P.

În continuare, am utilizat baza de date MaxMind pentru a asocia adresele participanților I2P cu sistemele autonome (ASN - Autonomous System Number) și țările din care provin.

Deoarece aproximativ jumătate dintre participanții observați sunt asociați cu mai multe adrese IP, după cum am arătat în Secțiunea 5.2.2, a fost necesară o metodă adecvată de numărare a participanților în fiecare ASN și stat. Pentru fiecare participant asociat cu mai multe adrese IP, am convertit toate aceste adrese în ASN-uri și țări înainte de efectuarea numărătorii, pentru a evita înregistrarea multiplă a aceluiași participant.

Dacă două adrese IP ale aceluiași participant aparțin aceluiași ASN sau aceluiași stat, participantul este numărat o singură dată. În schimb, dacă adresele aparțin unor ASN-uri sau țări diferite, fiecare asociere distinctă este contabilizată separat.

Figura 10 prezintă primele 20 de locații geografice în care sunt prezenți participanții I2P.

Statele Unite, Rusia, Anglia, Franța, Canada și Australia însumează peste 40% dintre participanții rețelei. Statele Unite ocupă primul loc, cu aproximativ 28.000 de participanți.

Cu excepția Noii Zeelande, toate statele membre ale alianței Five Eyes se regăsesc în primele zece poziții. Acest grup de 20 de țări reprezintă peste 60% din totalul participanților observați, restul provenind din alte 205 țări și teritorii.

Dintre cele 32 de state cu scoruri reduse în ceea ce privește libertatea presei (scor mai mare de 50), 30 sunt reprezentate în rețeaua I2P și însumează aproximativ 6.000 de participanți.

China conduce acest grup cu peste 2.000 de participanți, urmată de:

- Singapore, cu aproximativ 700 de participanți;
- Turcia, cu aproximativ 600 de participanți.

Având în vedere că autoritățile chineze blochează în mod activ accesul la Tor și la numeroase servicii VPN, este posibil ca o parte dintre utilizatorii chinezi să folosească I2P ca alternativă.

Numărul utilizatorilor din China ar putea crește dacă în rețea ar deveni disponibile mai multe servicii outproxy stabile. Deși China se numără printre țările în care participanții I2P sunt configurați implicit în modul hidden, operatorii routerelor pot dezactiva această setare pentru a face routerul mai accesibil și, implicit, mai performant.

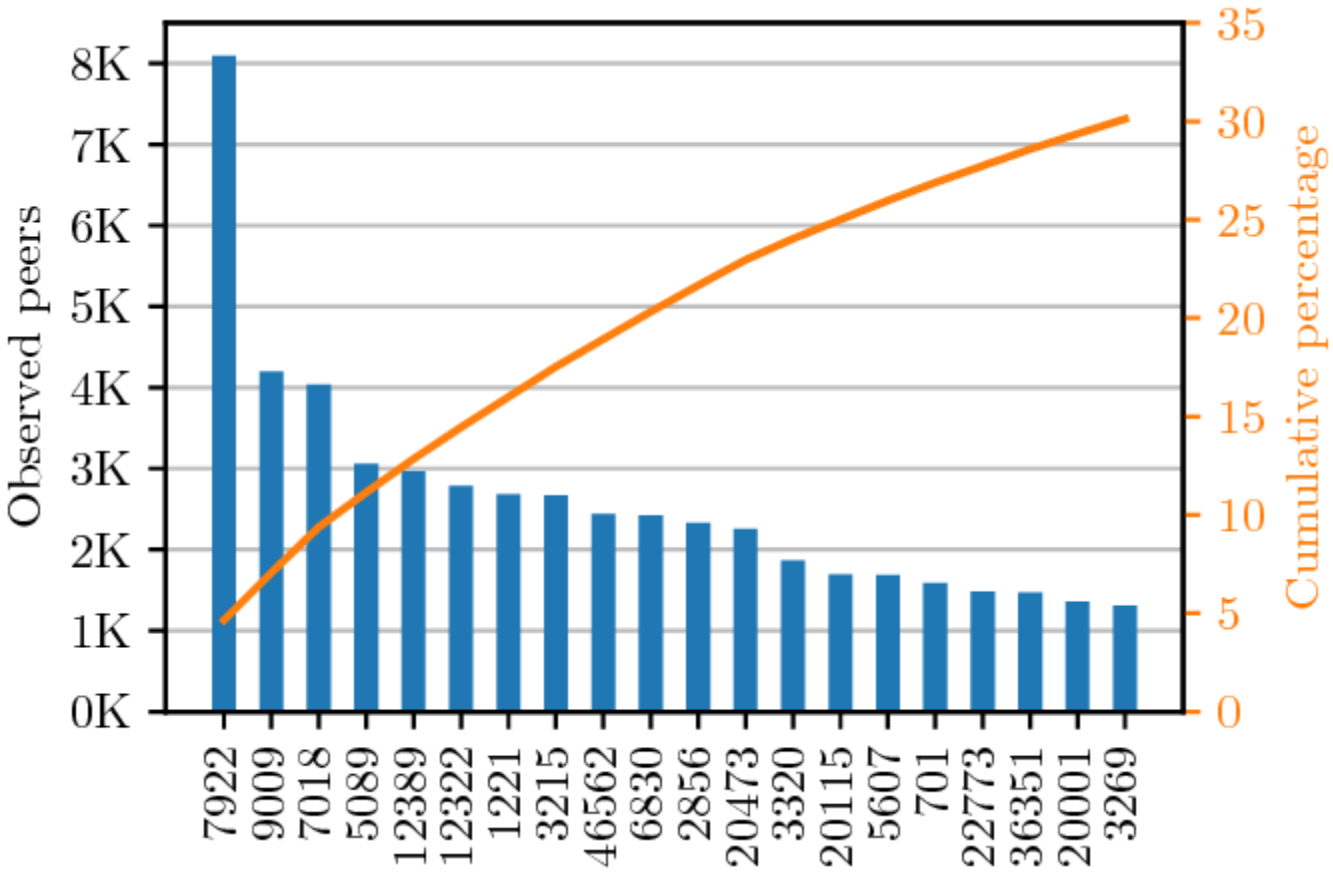

Figura 11. Primele 20 de sisteme autonome în care se află participanții I2P (axa X reprezintă numărul AS).

Figura 11 prezintă cele 20 de sisteme autonome din care provin cele mai multe adrese observate.

AS7922 (Comcast Cable Communications, LLC) ocupă primul loc, cu peste 8.000 de participanți.

Împreună, aceste 20 de sisteme autonome reprezintă peste 30% din totalul participanților observați.

După cum am menționat în Secțiunea 5.2.2, 58,9% dintre participanți își schimbă adresa IP cel puțin o dată. Am fost interesați să analizăm acest fenomen și din perspectivă geografică.

Prin asocierea adreselor IP cu ASN-uri și țări, am constatat că majoritatea participanților rămân în același sistem autonom sau în aceeași regiune geografică, chiar dacă utilizează mai multe adrese IP. Această observație este firească, deoarece furnizorii de servicii Internet schimbă frecvent adresele IP ale conexiunilor rezidențiale, însă acestea aparțin de regulă acelorași subrețele.

Totuși, am observat și un grup restrâns de participanți care își schimbă în mod repetat adresele IP între sisteme autonome și țări diferite.

Valorile maxime observate au fost:

- 39 de sisteme autonome diferite asociate unui singur participant;
- 25 de țări diferite asociate unui singur participant.

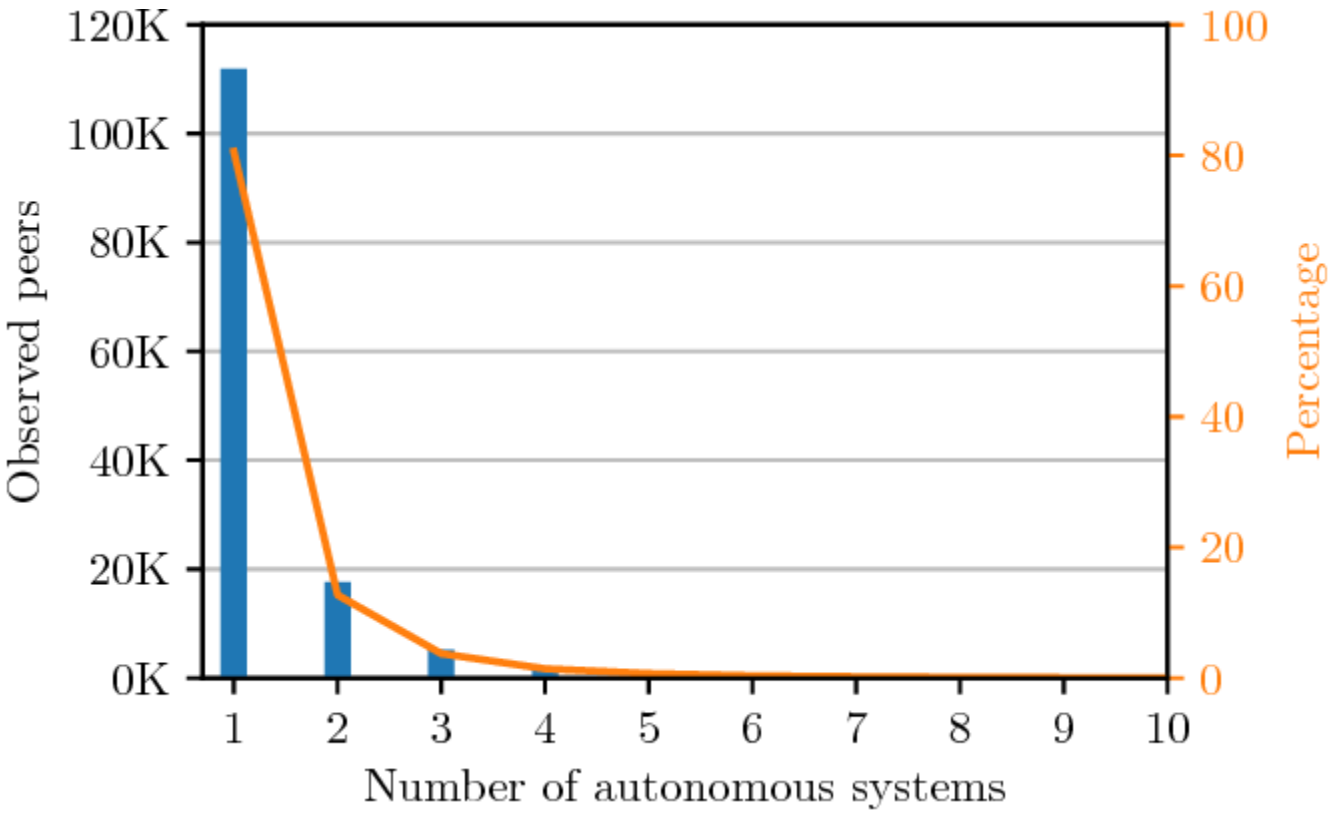

Figura 12. Numărul de sisteme autonome în care se regăsesc participanții asociați cu mai multe adrese IP.

Figura 12 arată distribuția participanților în funcție de numărul de sisteme autonome cu care sunt asociați.

Rezultatele indică faptul că:

- peste 80% dintre participanți sunt asociați cu un singur ASN;
- 8,4% sunt asociați cu mai mult de zece ASN-uri diferite.

În urma discuțiilor cu unul dintre dezvoltatorii I2P, o explicație posibilă pentru acest fenomen este faptul că anumite routere I2P funcționează în spatele unor servicii VPN sau Tor, ceea ce conduce la asocierea lor cu mai multe sisteme autonome.

Trebuie menționat că utilizatorii distribuției Tails (până la versiunea 2.11) puteau utiliza I2P prin intermediul rețelei Tor, această funcționalitate fiind inclusă oficial.

O limitare a utilizării bazei de date MaxMind este faptul că aproximativ 2.000 de adrese IP nu au putut fi asociate cu niciun ASN sau cu nicio țară folosind acest set de date.

Acest lucru nu înseamnă însă că nu am putut identifica 2.000 de participanți. Rezultatele prezentate în Secțiunea 5.2.2 arată că peste 55% dintre participanții cu adresă IP cunoscută sunt asociați cu mai multe adrese IP. Prin urmare, numărul real al participanților pentru care nu am putut determina ASN-ul și țara este limitat la cei care sunt asociați exclusiv cu o singură adresă IP care nu a putut fi rezolvată.

După cum am explicat în secțiunea dedicată considerațiilor etice, nu utilizăm API-uri publice de geolocalizare, chiar dacă acestea sunt mai precise, pentru a evita expunerea datelor și a proteja confidențialitatea participanților.

6. REZISTENȚA LA CENZURĂ

Din cauza arhitecturii centralizate a rețelei Tor, este relativ ușor pentru un cenzor să identifice și să blocheze toate routerele Tor publice. Pentru a reduce această vulnerabilitate, numeroase studii s-au concentrat asupra îmbunătățirii rezistenței Tor la blocare. În ciuda arhitecturii sale descentralizate, și I2P este susceptibilă la cenzură. Totuși, din câte știm, rezistența acestei rețele la cenzură nu a fost analizată în profunzime. În această secțiune ne concentrăm asupra acestui aspect.

6.1. Blocarea serverelor Reseed

Cunoscând mecanismul de inițializare (*bootstrapping*) al I2P, un cenzor poate bloca cu ușurință accesul la serverele reseed, dezactivând astfel procesul de conectare inițială la rețea. În consecință, serverele *reseed* reprezintă un punct unic de vulnerabilitate, într-un mod similar serverelor de directoare Tor, așa cum s-a întâmplat atunci când acestea au fost blocate în China în 2009.

În arhitectura actuală a I2P, un participant nou nu se poate conecta la restul rețelei dacă nu poate realiza procesul de *bootstrapping* prin intermediul unor servere *reseed*.

În aprilie 2017, pe forumul dezvoltatorilor I2P a fost publicat un mesaj în care se afirma că serverele *reseed* erau blocate în China. Am încercat să verificăm accesibilitatea serverelor *reseed* predefinite din mai multe puncte de observație aflate în China și am constatat că unele dintre acestea erau încă accesibile.

Mai mult, analiza prezentată în Secțiunea 5.3 arată că China se numără printre primele 20 de țări în care se află cei mai mulți participanți I2P. Un studiu anterior oferă două explicații posibile pentru această observație.

Prima posibilitate este ca raportul să fi descris o blocare limitată, aplicată doar de anumiți furnizori regionali de servicii Internet, și nu o blocare uniformă la nivel național.

A doua posibilitate este faptul că Marele Firewall al Chinei (*Great Firewall of China – GFW*) nu reușește întotdeauna să blocheze în mod consecvent toate destinațiile pe care încearcă să le filtreze.

Trebuie remarcat că, în prezent, I2P funcționează în cea mai mare parte a timpului ca o rețea autonomă, din cauza disponibilității

intermitente a serviciilor outproxy. În plus, deoarece rețeaua este încă relativ mică, este posibil să nu fi devenit încă o țintă prioritară pentru GFW. Totuși, pe măsură ce rețeaua se va extinde și va beneficia de un suport mai stabil din partea serviciilor outproxy către Internetul public, blocarea la scară largă va deveni probabil inevitabilă.

Dezvoltatorii I2P au anticipat scenariul în care toate serverele *reseed* ar putea fi blocate. Din acest motiv, software-ul routerului I2P include o funcție integrată care permite realizarea unui proces de *reseed* manual.

Prin intermediul acestei funcționalități, orice participant I2P activ poate deveni un furnizor manual de date *reseed*. Mai exact, funcția poate genera un fișier de tip i2pseeds.su3. Acest fișier poate fi distribuit altor participanți care nu au acces la serverele *reseed* necesare procesului de inițializare.

Distribuirea poate fi realizată prin canale secundare, într-un mod asemănător mecanismului prin care Tor distribuie nodurile bridge, folosind de exemplu:

- e-mail;
- servicii de partajare a fișierelor;
- alte canale externe de distribuție.

Într-un asemenea scenariu, un cenzor care dorește să împiedice utilizatorii locali să acceseze I2P trebuie să identifice și să blocheze adresele tuturor participanților activi din rețea.

Totuși, deoarece I2P este o rețea P2P distribuită, obținerea unei imagini complete asupra întregii rețele este o sarcină dificilă.

În secțiunea următoare analizăm eficiența și costul unei astfel de strategii de blocare bazate pe adrese.

6.2. Blocarea probabilistică bazată pe adrese

Pornim de la scenariul în care un cenzor încearcă să monitorizeze rețeaua și să colecteze informații despre participanții activi (adică adresele IP și porturile utilizate), pentru a putea împiedica utilizatorii locali să acceseze rețeaua. În continuare evaluăm atât rezistența unui participant I2P la blocare, cât și gradul de utilizabilitate al rețelei sub presiunea unei campanii agresive de blocare.

6.2.1. Configurația experimentală

Modelul probabilistic de blocare este alcătuit din:

1. un grup de routere de monitorizare operate de cenzor (de exemplu un furnizor de servicii Internet sau o autoritate guvernamentală);
2. o victimă pe care cenzorul încearcă să o împiedice să acceseze I2P.

Prin operarea unor routere în rețea, cenzorul poate obține informații despre o mare parte dintre participanții cu care victima ar putea avea nevoie să comunice pentru a accesa rețeaua. În acest fel, cenzorul poate împiedica accesul victimei la I2P.

Rata de blocare este calculată ca proporția adreselor IP ale participanților observate în netDb-ul victimei care se regăsesc și în netDb-ul routerelor controlate de cenzor.

6.2.2. Evaluarea rezistenței la blocare

Luăm în considerare un nod I2P de lungă durată, care participă de mult timp la rețea și acumulează un număr mare de obiecte RouterInfo în baza sa locală netDb, urmând să fie supus blocării.

Pentru simularea cenzorului, folosim adresele IP ale participanților activi zilnic observate de cele 20 de routere aflate sub controlul nostru. În rolul victimei folosim un router independent, operat în afara infrastructurii care găzduiește cele 20 de routere de monitorizare.

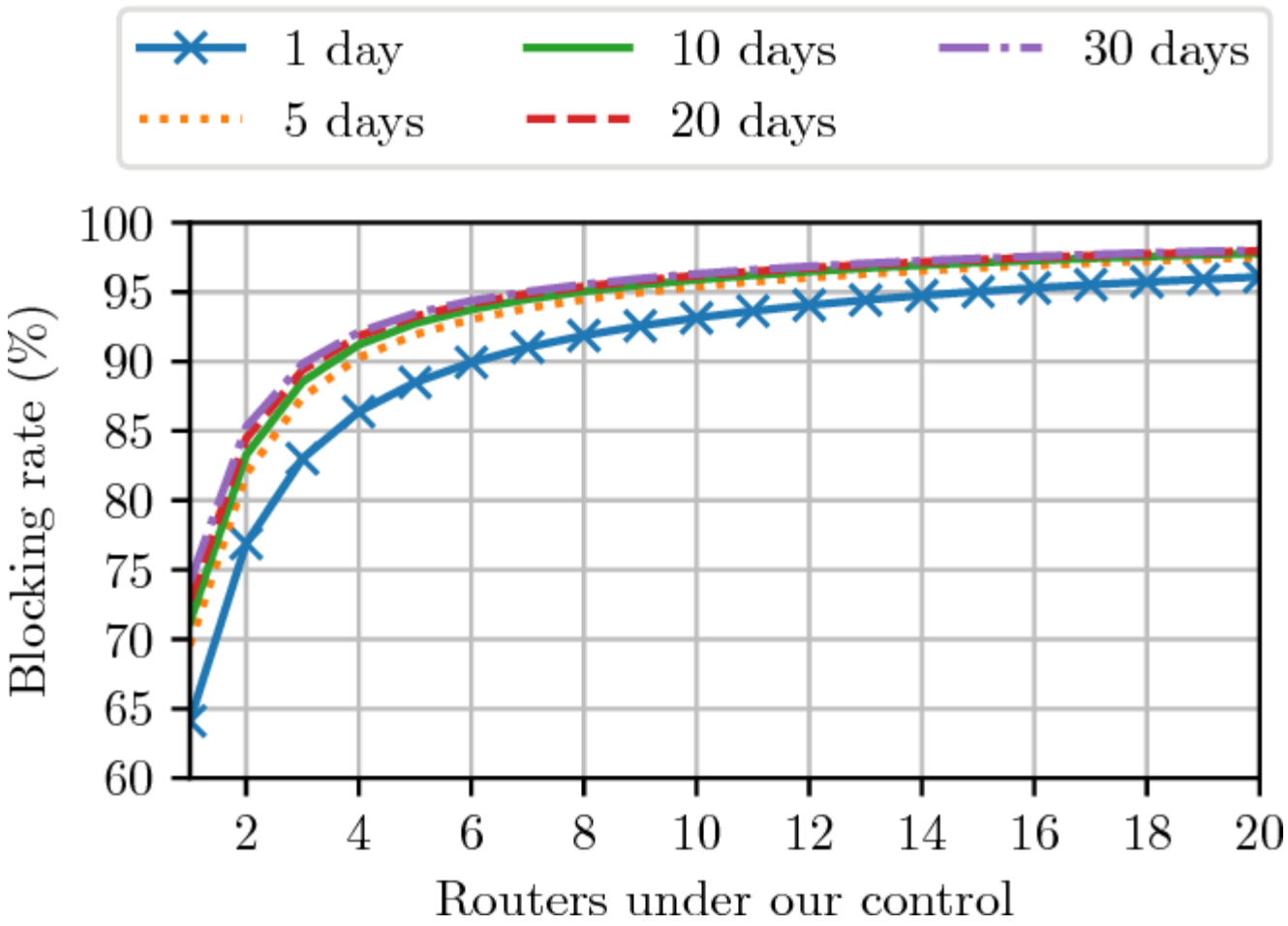

Figura 13. Ratele de blocare pentru diferite intervale de păstrare a listelor negre.

Linia albastră (cea mai de jos) din Figura 13 prezintă rata cumulată de blocare obținută de un adversar care operează între 1 și 20 de routere timp de o singură zi.

Rezultatele arată că:

- prin operarea a 20 de routere, un cenzor poate bloca peste 95% dintre adresele IP cunoscute victimei;
- prin operarea a doar 6 routere poate bloca deja aproximativ 90% dintre aceste adrese.

Aceste valori sunt calculate presupunând că cenzorul folosește exclusiv adresele IP colectate într-o singură zi. În practică, situația poate fi chiar mai gravă.

Studii anterioare asupra rețelei Tor au arătat că, odată ce o adresă IP este identificată ca participantă la o rețea anonimă sau ca releu de comunicații (de exemplu server VPN), aceasta poate rămâne pe listele negre timp de câteva zile sau chiar mai mult de o lună.

Folosind rezultatele analizei fluctuației participanților prezentate în Secțiunea 5.2, am evaluat impactul extinderii perioadei de păstrare a adreselor IP pe lista neagră la: 5 zile; 10 zile; 20 de zile; 30 de zile. Am constatat că:

- extinderea perioadei de blocare de la o zi la cinci zile crește rata de blocare la peste 97% atunci când sunt operate 20 de routere;
- aceeași rată poate atinge aproximativ 95% chiar și cu doar 10 routere.

În cazul unor perioade de: 10 zile; 20 de zile; 30 de zile, rata de blocare depășește 98% atunci când sunt folosite 20 de routere și ajunge la aproximativ 96% chiar și cu doar 10 routere.

După cum arată Figura 13, o perioadă de numai cinci zile este suficientă pentru a obține o rată foarte ridicată de blocare. Această cerință se încadrează cu ușurință în capacitățile firewall-urilor performante utilizate pentru cenzură la nivel național, care pot gestiona fără dificultate un număr atât de mare de reguli.

6.2.3. Evaluarea utilizabilității rețelei

Deoarece mecanismul de blocare bazat pe adrese utilizat de Marele Firewall al Chinei folosește tehnica null routing, prin care pachetele nedorite sunt direcționate către un router de tip *black hole*, am configurat routerul nostru upstream astfel încât să elimine silențios toate pachetele care conțin adrese IP ale participanților I2P observați în cadrul studiului.

Am creat apoi trei *eepsites* experimentale pentru a analiza impactul blocării bazate pe adrese asupra timpului de încărcare a paginilor.

Aceste site-uri au fost construite folosind fișiere HTML foarte simple și de dimensiuni reduse pentru a evita consumul inutil de resurse ale rețelei. De asemenea, am utilizat propriile noastre eepsites și nu site-uri publice cunoscute, pentru a ne asigura că experimentul nu afectează utilizatorii legitimi.

Mai întâi am măsurat timpul normal de încărcare al acestor site-uri. Rezultatele prezentate în Figura 13 indică faptul că un cenzor poate bloca între aproximativ 65% și 98% dintre adresele participanților prezente în netDb-ul victimei.

Ulterior, am accesat fiecare *eepsite* de zece ori pentru fiecare rată de blocare analizată, măsurând: timpul de încărcare al paginii; numărul cererilor expirate (*timeout*); numărul răspunsurilor HTTP 504.

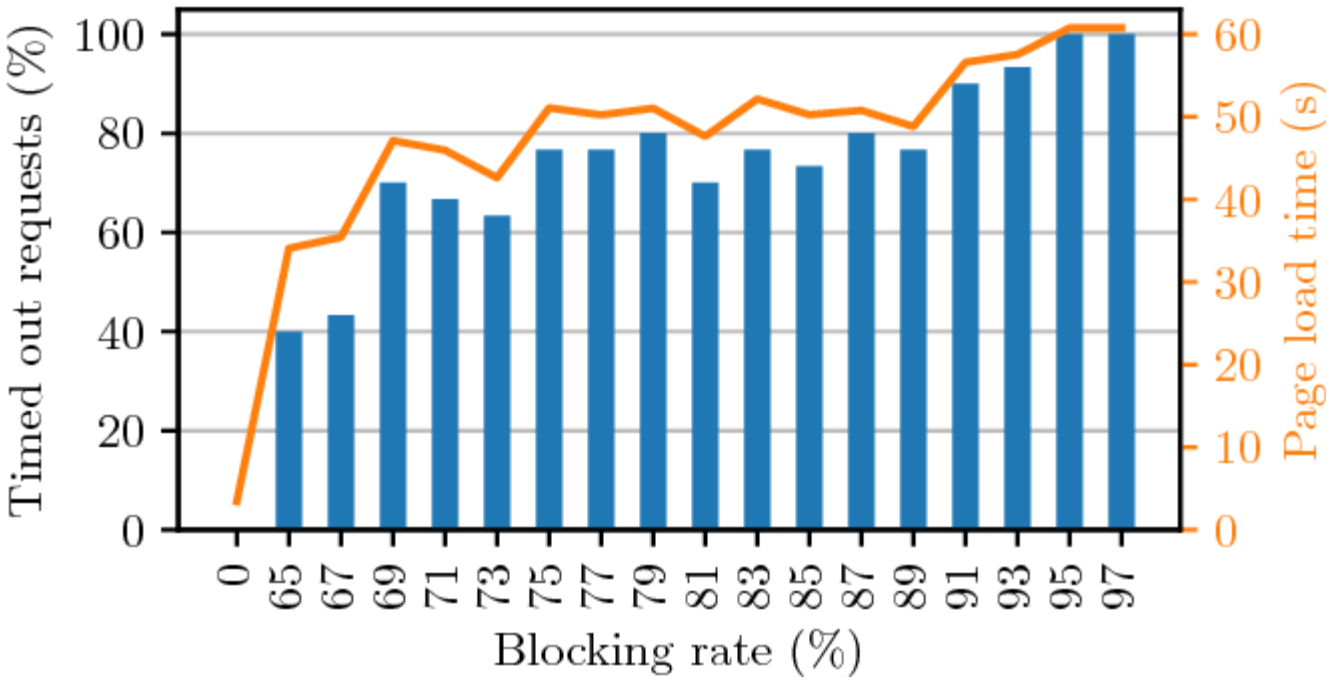

Figura 14. Procentul cererilor expirate și latența încărcării paginilor în condiții de blocare.

Figura 14 arată că timpul mediu de încărcare al eepsites-urilor noastre este de 3,4 secunde în absența oricărei blocări.

Atunci când sunt blocați 65% dintre participanți: latența depășește 20 de secunde; aproximativ 40% dintre cereri expiră.

Pentru rate de blocare cuprinse între 70% și 90%: timpul de încărcare depășește frecvent 40 de secunde; peste 60% dintre cereri expiră.

În cazul unor rate de blocare mai mari de 90%, utilitatea rețelei se degradează sever: între 95% și 100% dintre cereri expiră; accesarea serviciilor devine practic imposibilă.

Rezultatele arată că, deși I2P este o rețea descentralizată, blocarea unei proporții suficient de mari dintre participanți poate reduce dramatic performanța și poate face rețeaua aproape inutilizabilă pentru utilizatorii obișnuiți.

7. DISCUȚII

7.1. Soluții potențiale împotriva blocării

Pe măsură ce tot mai multe regimuri autoritare încearcă să împiedice utilizatorii locali să acceseze rețeaua Tor, proiectul Tor pune la dispoziția utilizatorilor din regiunile restricționate un set special de relee denumite bridge-uri. În mod similar, I2P ar putea adopta utilizarea bridge-urilor pentru a facilita accesul utilizatorilor supuși cenzurii, în combinație cu noul model de trafic rezistent la amprentare (*non-fingerprintable*), aflat în prezent în dezvoltare.

În timp ce comunitatea Tor întâmpină dificultăți în recrutarea și menținerea bridge-urilor deoarece acestea sunt adesea descoperite și blocate rapid, I2P are un potențial mai mare pentru adoptarea unei astfel de soluții datorită ratei ridicate de fluctuație a participanților din rețeaua sa dinamică și descentralizată.

În ciuda ratelor de blocare ridicate prezentate în Secțiunea 6.2, am observat că o parte dintre adresele IP ale participanților nu pot fi blocate. Aceste adrese aparțin, de regulă, participanților nou conectați la rețea. Din acest motiv, o posibilă soluție ar fi utilizarea acestor participanți drept bridge-uri pentru utilizatorii aflați în medii cenzurate. Fiind recent intrați în rețea, este mai puțin probabil ca aceștia să fie identificați și blocați imediat de către cenzor.

Totuși, utilizarea exclusivă a participanților nou conectați ca bridge-uri poate reprezenta doar o soluție temporară pentru utilizatorii care au nevoie de acces la I2P pe termen scurt. Dacă acești participanți rămân suficient timp în rețea, routerele de

monitorizare operate de cenzor îi vor identifica și îi vor bloca în cele din urmă.

O abordare care ar putea remedia această problemă este combinarea participanților nou conectați cu participanții firewalled identificați în Secțiunea 5.1, pentru a obține o metodă mai durabilă de evitare a cenzurii.

Conform Figurii 6, există aproximativ 14.000 de participanți *firewalled* activi zilnic în rețea. În lipsa unei adrese IP publice, asupra acestora nu poate fi aplicată tehnica de blocare bazată pe adrese descrisă în Secțiunea 6.2.

În arhitectura actuală a I2P, probabilitatea ca un cenzor să descopere adresa IP a unui participant firewalled depinde de probabilitatea ca routerele aflate sub controlul cenzorului:

1. să fie selectate ca introducers pentru acel participant;
2. să interacționeze direct cu participantul respectiv.

Cu excepția infrastructurii necesare colectării și distribuirii bridge-urilor, soluția propusă nu introduce costuri suplimentare semnificative pentru ceilalți participanți.

Întrucât majoritatea participanților activi sunt selectați implicit pentru a contribui la rutarea traficului altor utilizatori, abordarea descrisă modifică doar modul în care utilizatorii supuși cenzurii selectează participanți neblocați pentru a accesa restul rețelei.

În consecință, utilizarea combinată a participanților nou conectați și a participanților firewalled poate reprezenta o soluție viabilă și relativ sustenabilă pentru utilizatorii care au nevoie de acces pe termen lung la rețea.

7.2. De la blocare la alte tipuri de atacuri

Deși acest studiu se concentrează asupra problemei blocării accesului la I2P, modelul probabilistic de blocare pe care l-am introdus nu se limitează doar la împiedicarea accesului la rețea.

Dacă un cenzor nu reușește să blocheze complet accesul unui utilizator local, acesta poate recurge la alte tipuri de atacuri, precum analiza traficului, pentru a compromite anonimatul utilizatorului. De exemplu, poate încerca să determine ce destinații sunt accesate de acesta.

Un scenariu posibil este următorul. După blocarea a peste 95% dintre participanții activi ai rețelei, atacatorul poate introduce în rețea propriile routere malițioase. Acesta configurează apoi firewall-ul local astfel încât victima să fie forțată să utilizeze aceste routere pentru a comunica cu restul rețelei I2P.

În această situație, procesul de inițializare al victimei are loc efectiv în interiorul infrastructurii controlate de atacator.

Atacatorul poate facilita acest proces prin includerea propriilor routere pe o listă albă (*whitelist*), în timp ce continuă să blocheze în mod repetat adresele celorlalți participanți activi.

Prin restrângerea artificială a imaginii pe care victima o are asupra rețelei, atacatorul se apropie de realizarea mai multor tipuri de atacuri, inclusiv a atacurilor de deanomimizare menționate anterior**.**

8. Concluzii

În această lucrare am realizat un studiu de măsurare destinat unei mai bune înțelegeri a rețelei de anonimitate I2P, ceea ce ne-a permis ulterior să evaluăm rezistența acesteia la cenzură.

Deși I2P nu este la fel de populară ca Tor, în principal deoarece funcționează în mare măsură ca o rețea de anonimitate autonomă, rezultatele măsurătorilor noastre arată că dimensiunea rețelei s-a menținut constantă pe parcursul celor trei luni de studiu, existând aproximativ 32.000 de participanți activi zilnic.

Dintre aceștia, aproximativ 14.000 se conectează la rețeaua I2P din spatele unor dispozitive NAT sau firewall-uri.

Pe durata celor trei luni de analiză am identificat și un grup de aproximativ 6.000 de participanți proveniți din țări cu scoruri reduse privind libertatea presei.

Rezultatele noastre arată că un cenzor poate împiedica relativ ușor utilizatorii locali să acceseze rețeaua I2P, în ciuda caracterului său descentralizat și cu costuri relativ reduse.

Deși victima utilizată în evaluarea noastră este presupusă a fi un participant puternic și de lungă durată, care participă neîntrerupt la rețea, am demonstrat că un cenzor poate bloca totuși peste 95% dintre adresele IP prezente în baza sa netDb.

O asemenea rată de blocare poate fi obținută prin operarea a doar 10 routere în rețea. Prin utilizarea unor perioade mai lungi de păstrare a listelor negre și prin operarea unui număr mai mare de routere (de exemplu 20), cenzorul poate ajunge la o rată de blocare apropiată de 100%.

Ca direcție de cercetare viitoare, intenționăm să extindem acest studiu prin evaluarea viabilității utilizării participanților nou

conectați împreună cu participanții firewalled ca bridge-uri pentru utilizatorii care sunt împiedicați să acceseze rețeaua.

• Acknowledgments We would like to thank our shepherd, Mirja Kühlewind, the anonymous reviewers, and the following members of the I2P team for their valuable feedback: Sadie Doreen, str4d, echelon, meeh, psi, slumlord, and zzz. References

• (1) Ali et al. (2016)Afzaal Ali, Maria Khan, Muhammad Saddique, Umar Pirzada, Muhammad Zohaib, Imran Ahmad, and Narayan Debnath. 2016.TOR vs I2P: A Comparative Study. In Proceedings of the 2016 IEEE International Conference on Industrial Technology.

• Biryukov et al. (2014)A. Biryukov, I. Pustogarov, F. Thill, and R. P. Weinmann. 2014.Content and Popularity Analysis of Tor Hidden Services. In 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW). 188–193.

• Biryukov et al. (2013)A. Biryukov, I. Pustogarov, and R. P. Weinmann. 2013.Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. In 2013 IEEE Symposium on Security and Privacy. 80–94.

• Bloomberg (7 10)Bloomberg. 2017-07-10.China Tells Carriers to Block Access to Personal VPNs by February.https://www.bloomberg.com/news/articles/2017-07-

10/china-is-said-to-order-carriers-to-bar-personal-vpns-by-february

• Cate Cadell (7 29)Cate Cadell. 2017-07-29.Apple says it is removing VPN services from China App Store.Reuters.https://www.reuters.com/article/us-china-apple-vpn/apple-says-it-is-removing-vpn-services-from-china-app-store-idUSKBN1AE0BQ

• Choffnes et al. (2017)David Choffnes, Phillipa Gill, and Alan Mislove. 2017.An Empirical Evaluation of Deployed DPI Middleboxes and Their Implications for Policymakers. In Proceedings of Research Conference on Communications, Information and Internet Policy.

• Conrad and Shirazi (2014)Bernd Conrad and Fatemeh Shirazi. 2014.A Survey on Tor and I2P. In Proceedings of the 9th International Conference on Internet Monitoring and Protection (ICIMP 2014).

• Dingledine (2000)Roger Dingledine. 2000.The Free Haven Project: design and deployment of an anonymous secure data haven.Master's thesis. MIT, Dept. of Electrical Engineering and Computer Science.

• Dingledine et al. (2001)Roger Dingledine, Michael J. Freedman, and David Molnar. 2001.The Free Haven Project: Distributed Anonymous Storage Service. In International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability. Springer-Verlag, Berlin, Heidelberg, 67–95.http://dl.acm.org/citation.cfm?id=371931.371978

• Dingledine et al. (2004)R. Dingledine, N. Mathewson, and P. Syverson. 2004.Tor: The Second-Generation Onion Router. In Proceedings of the 13th USENIX Security Symposium). 303–319.

• Dunna et al. (2018)Arun Dunna, Ciarán O'Brien, and Phillipa Gill. 2018.Analyzing China's Blocking of Unpublished Tor Bridges. In 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18). USENIX Association, Baltimore, MD.https://www.usenix.org/conference/foci18/presentation/dunna

• Dutton (2011)William H Dutton. 2011.Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet.UNESCO.

• Ensafi et al. (2015a)Roya Ensafi, David Fifield, Philipp Winter, Nick Feamster, Nicholas Weaver, and Vern Paxson. 2015a.Examining How the Great Firewall Discovers Hidden Circumvention Servers. In Proceedings of the 2015 ACM Conference on Internet Measurement Conference - IMC '15. ACM Press, New York, USA, 445–458.

• Ensafi et al. (2015b)Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R Crandall. 2015b.Analyzing the Great Firewall of China over space and time.Proceedings on privacy enhancing technologies 2015, 1 (2015), 61–76.

• Erika McCallister, Tim Grance, Karen Scarfone (2010)Erika McCallister, Tim Grance, Karen Scarfone. 2010.Guide to Protecting the Confidentiality of Personally

Identifiable Information.National Institute of Standards and Technology, U.S. Department of Comerece.

• Fifield and Tsai (2016)David Fifield and Lynn Tsai. 2016.Censors' Delay in Blocking Circumvention Proxies. In 6th USENIX Workshop on Free and Open Communications on the Internet (FOCI 16). USENIX Association, Austin, TX.

• Freedman ([n. d.])Michael J Freedman. [n. d.].Design and analysis of an anonymous communication channel for the free haven project.

• Freedom House (2017)Freedom House. 2017.Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy.https://freedomhouse.org/report/freedom-net/freedom-net-2017

• Gao et al. (2017)Yue Gao, Qingfeng Tan, Jinqiao Shi, Xuebin Wang, and Muqian Chen. 2017.Large-scale discovery and empirical analysis for I2P eepSites. In 2017 IEEE Symposium on Computers and Communications (ISCC). 444–449.

• Goldschlag et al. (1996)David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. 1996.Hiding Routing information. In Information Hiding, Ross Anderson (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 137–150.

• Grigg (2017)Jack Grigg. 2017.Looking For Group: Open Research Questions about I2P. In 10th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs).

• Herrmann and Grothoff (2011)Michael Herrmann and Christian Grothoff. 2011.Privacy-implications of performance-

based peer selection by onion-routers: a real-world case study using I2P. In International Symposium on Privacy Enhancing Technologies Symposium. Springer, 155–174.

• Hoang and Pishva (2014)Nguyen Phong Hoang and Davar Pishva. 2014.Anonymous Communication and Its Importance in Social Networking.. In The 16th International Conference on Advanced Communication Technology (ICACT). IEEE, 34–39.https://doi.org/10.1109/ICACT.2014.6778917

• I2P Official Homepage (2010)I2P Official Homepage. 2010.Threat Models.https://geti2p.net/en/docs/how/threat-model

• I2P Official Homepage (2011)I2P Official Homepage. 2011.I2P Tunnel Routing.https://geti2p.net/en/docs/how/tunnel-routing

• I2P Official Homepage (1 03)I2P Official Homepage. 2014-01-03.NTCP Obfuscation.https://geti2p.net/spec/proposals/106-ntcp-obfuscation

• I2P Official Homepage (2017)I2P Official Homepage. 2017.A Gentle Introduction to How I2P Works.https://geti2p.net/en/docs/how/intro

• I2P Official Homepage (2018a)I2P Official Homepage. 2018a.Common Structures Specification - Router Address.https://geti2p.net/spec/common-structures#struct-routeraddress

• I2P Official Homepage (2018b)I2P Official Homepage. 2018b.Frequently Asked Questions.https://geti2p.net/en/faq#badcontent

Mulțumiri

• Dorim să îi mulțumim coordonatoarei lucrării noastre, Mirja Kühlewind, recenzenților anonimi și următorilor membri ai echipei I2P pentru feedbackul valoros oferit:

• Sadie Doreen

• str4d

• echelon

• meeh

• psi

• slumlord

• zzz

• Referințe

• Ali et al. (2016)
Afzaal Ali, Maria Khan, Muhammad Saddique, Umar Pirzada, Muhammad Zohaib, Imran Ahmad și Narayan Debnath. 2016. *TOR vs I2P: A Comparative Study*. În *Proceedings of the 2016 IEEE International Conference on Industrial Technology*.

• Biryukov et al. (2014)
A. Biryukov, I. Pustogarov, F. Thill și R. P. Weinmann. 2014. *Content and Popularity Analysis of Tor Hidden Services*. În

2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 188-193.

- Biryukov et al. (2013)

A. Biryukov, I. Pustogarov și R. P. Weinmann. 2013. *Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization*. În *2013 IEEE Symposium on Security and Privacy*, pp. 80-94.

- Bloomberg (10.07.2017)

Bloomberg. 2017. *China Tells Carriers to Block Access to Personal VPNs by February*. https://www.bloomberg.com/news/articles/2017-07-10/china-is-said-to-order-carriers-to-bar-personal-vpns-by-february

- Cate Cadell (29.07.2017)

Cate Cadell. 2017. *Apple spune că elimină serviciile VPN din App Store-ul din China*. Reuters. https://www.reuters.com/article/us-china-apple-vpn/apple-says-it-is-removing-vpn-services-from-china-app-store-idUSKBN1AE0BQ

- Choffnes et al. (2017)

David Choffnes, Phillipa Gill și Alan Mislove. 2017. *An Empirical Evaluation of Deployed DPI Middleboxes and Their Implications for Policymakers*. În *Proceedings of Research Conference on Communications, Information and Internet Policy*.

- Conrad și Shirazi (2014)

Bernd Conrad și Fatemeh Shirazi. 2014. *A Survey on Tor and I2P*. În *Proceedings of the 9th International Conference on Internet Monitoring and Protection (ICIMP 2014)*.

- Dingledine (2000)

Roger Dingledine. 2000. *The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven*. Lucrare de masterat. MIT, Department of Electrical Engineering and Computer Science.

- Dingledine, Freedman și Molnar (2001)

Roger Dingledine, Michael J. Freedman și David Molnar. 2001. *The Free Haven Project: Distributed Anonymous Storage Service*. În *International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability*. Springer-Verlag, Berlin, Heidelberg, pp. 67-95. http://dl.acm.org/citation.cfm?id=371931.371978

- Dingledine et al. (2004)

R. Dingledine, N. Mathewson și P. Syverson. 2004. *Tor: The Second-Generation Onion Router*. În *Proceedings of the 13th USENIX Security Symposium*, pp. 303-319.

- Dunna et al. (2018)

Arun Dunna, Ciarán O'Brien și Phillipa Gill. 2018. *Analyzing China's Blocking of Unpublished Tor Bridges*. În *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*. USENIX Association, Baltimore, Maryland. https://www.usenix.org/conference/foci18/presentation/dunna

- Dutton (2011)

William H. Dutton. 2011. *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*. UNESCO.

- Ensafi et al. (2015a)

Roya Ensafi, David Fifield, Philipp Winter, Nick Feamster, Nicholas Weaver și Vern Paxson. 2015. *Examining How the Great Firewall Discovers Hidden Circumvention Servers*. În *Proceedings of the 2015 ACM Internet Measurement Conference (IMC '15)*. ACM Press, New York, pp. 445-458.

- Ensafi et al. (2015b)

Roya Ensafi, Philipp Winter, Abdullah Mueen și Jedidiah R. Crandall. 2015. *Analyzing the Great Firewall of China over Space and Time*. *Proceedings on Privacy Enhancing Technologies*, 2015(1), pp. 61-76.

- McCallister, Grance și Scarfone (2010)

Erika McCallister, Tim Grance și Karen Scarfone. 2010. *Guide to Protecting the Confidentiality of Personally Identifiable Information*. National Institute of Standards and Technology, U.S. Department of Commerce.

- Fifield și Tsai (2016)

David Fifield și Lynn Tsai. 2016. *Censors' Delay in Blocking Circumvention Proxies*. În *6th USENIX Workshop on Free and Open Communications on the Internet (FOCI 16)*. USENIX Association, Austin, Texas.

- Freedman ([f.d.])

Michael J. Freedman. *Design and Analysis of an Anonymous Communication Channel for the Free Haven Project*.

- Freedom House (2017). *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*. https://freedomhouse.org/report/freedom-net/freedom-net-2017

- Gao et al. (2017)

Yue Gao, Qingfeng Tan, Jinqiao Shi, Xuebin Wang și Muqian Chen. 2017. *Large-Scale Discovery and Empirical Analysis for I2P Eepsites*. În *2017 IEEE Symposium on Computers and Communications (ISCC)*, pp. 444-449.

- Goldschlag, Reed și Syverson (1996)

David M. Goldschlag, Michael G. Reed și Paul F. Syverson. 1996. *Hiding Routing Information*. În *Information Hiding*, Ross Anderson (ed.). Springer, Berlin, Heidelberg, pp. 137-150.

- Grigg (2017)

Jack Grigg. 2017. *Looking For Group: Open Research Questions about I2P*. În *10th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)*.

- Herrmann și Grothoff (2011)

Michael Herrmann și Christian Grothoff. 2011. *Implicațiile asupra confidențialității ale selecției nodurilor pe baza performanței: un studiu de caz real folosind I2P*. În *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 155-174.

- Hoang și Pishva (2014)

Nguyen Phong Hoang și Davar Pishva. 2014. *Comunicarea anonimă și importanța ei în rețelele sociale*. În *The 16th International Conference on Advanced Communication Technology (ICACT)*. IEEE, pp. 34-39. https://doi.org/10.1109/ICACT.2014.6778917

- **I2P Official Homepage (2018c)**
What Ports Does I2P Use?
https://geti2p.net/en/faq#ports

- **I2P Official Homepage (martie 2018)**
Secure Semireliable UDP (SSU).
https://geti2p.net/en/docs/transport/ssu#introduction

- **I2P Official Homepage (aprilie 2018a)**
Garlic Routing and "Garlic" Terminology.
https://geti2p.net/en/docs/how/garlic-routing

- **I2P Official Homepage (aprilie 2018b)**
I2P Academic Research Guidelines.
https://geti2p.net/en/research

- **I2P Official Homepage (aprilie 2018c)**
The Network Database of I2P.
https://geti2p.net/en/docs/how/network-database

- **I2P Official Homepage (14.05.2018)**
NTCP2.
https://geti2p.net/spec/proposals/111-ntcp-2

- **James Cox (2012)**
James Cox. 2012. *Canada and the Five Eyes Intelligence Community*. Canadian Defence and Foreign Affairs Institute.

- **Jeong et al. (2016)**
Seong Hoon Jeong, Ah Reum Kang, Joongheon Kim, Huy Kang Kim și Aziz Mohaisen. 2016. *A Longitudinal Analysis of .i2p Leakage in the Public DNS Infrastructure*. În *Proceedings of the 2016 ACM SIGCOMM Conference*, pp. 557-558.

- **Lah (2008)**
Frederick Lah. 2008. *Are IP Addresses Personally Identifiable Information? ISJLP*, vol. 4, p. 681.

- **Li et al. (2017)**

Fangfan Li, Abbas Razaghpanah, Arash Molavi Kakhki, Arian Akhavan Niaki, David Choffnes, Phillipa Gill și Alan Mislove. 2017. *Lib.erate (N): A Library for Exposing Traffic Classification Rules and Avoiding Them Efficiently*. În *Proceedings of the 2017 Internet Measurement Conference (IMC '17)*. ACM, New York, pp. 128-141.

- **Liu et al. (2014)**

Peipeng Liu, Lihong Wang, Qingfeng Tan, Quangang Li, Xuebin Wang și Jinqiao Shi. 2014. *Empirical Measurement and Analysis of I2P Routers*. *Journal of Networks*, 9(9), pp. 2269-2278.

- **Loesing et al. (2010)**

Karsten Loesing, Steven J. Murdoch și Roger Dingledine. 2010. *A Case Study on Measuring Statistical Data in the Tor Anonymity Network*. În *Proceedings of the Workshop on Ethics in Computer Security Research (WECSR 2010)*. Springer.

- **Marcello Mari (05.12.2014)**

Marcello Mari. *How Facebook's Tor Service Could Encourage a More Open Web*. *The Guardian*. https://www.theguardian.com/technology/2014/dec/05/how-faceboook-tor-service-encourage-open-web

- **Matic et al. (2017)**

Srdjan Matic, Carmela Troncoso și Juan Caballero. 2017. *Dissecting Tor Bridges: A Security Evaluation of Their Private and Public Infrastructures*. În *Network and Distributed Systems Security Symposium*, pp. 1-15.

- **Maymounkov și Mazieres (2002)**

Petar Maymounkov și D. Mazieres. 2002. *Kademlia: A Peer-to-Peer Information System Based on the XOR Metric*. În *First International Workshop on Peer-to-Peer Systems*, pp. 53-65.

- **McCoy et al. (2008)**

Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno și Douglas Sicker. 2008. *Shining Light in Dark Places: Understanding the Tor Network*. În *Privacy Enhancing Technologies*, eds. Nikita Borisov și Ian Goldberg. Springer, pp. 63-76.

- **Nobori și Shinjo (2014)**

D. Nobori și Y. Shinjo. 2014. *VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls*. În *11th USENIX Symposium on Networked Systems Design and Implementation*.

- **Palko Karasz (02.05.2018)**

Palko Karasz. *What Is Telegram, and Why Are Iran and Russia Trying to Ban It? The New York Times*. https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html

- **Reporters Without Borders (2018)**

World Press Freedom Index. https://rsf.org/en/ranking

- **Reseed Contributor (15.04.2017)**

Circumvent Blockade of Reseed Servers in China. I2P Development and Discussion Forum. http://zzz.i2p/topics/2302-request-for-comments-circumvent-blockade-of-reseed-servers-in-china

- **Shahbar și Zincir-Heywood (2017)**

Khalid Shahbar și A. Nur Zincir-Heywood. 2017. *Effects of Shared Bandwidth on Anonymity of the I2P Network Users*. În *Proceedings of the 38th IEEE Symposium on Security and Privacy Workshops, 2nd International Workshop on Traffic Measurements for Cybersecurity (WTMC 2017)*.

- **Sicker et al. (2007)**

Douglas C. Sicker, Paul Ohm și Dirk Grunwald. 2007. *Legal Issues Surrounding Monitoring During Network Research*. În *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement (IMC '07)*. ACM, New York, pp. 141-148.

- **Singh et al. (2017)**

Rachee Singh, Rishab Nithyanand, Sadia Afroz, Paul Pearce, Michael Carl Tschantz, Phillipa Gill și Vern Paxson. 2017. *Characterizing the Nature and Dynamics of Tor Exit Blocking*. În *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, pp. 325-341.

- **SonicWALL (11.05.2018)**

How to Block I2P Traffic Using App Control Advanced. https://support.sonicwall.com/kb/sw13993

- **Stuart Dredge (05.11.2013)**

What Is Tor? A Beginner's Guide to the Privacy Tool. *The Guardian*. https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

- **Sun et al. (2015)**

Yixin Sun, Anne Edmundson, Laurent Vanbever, Oscar Li, Jennifer Rexford, Mung Chiang și Prateek Mittal. 2015. *RAPTOR: Routing Attacks on Privacy in Tor*. În *24th USENIX Security Symposium (USENIX Security 15)*, pp. 271-286.

- **Syverson et al. (1997)**

P. F. Syverson, D. M. Goldschlag și M. G. Reed. 1997. *Anonymous Connections and Onion Routing*. În *IEEE Symposium on Security and Privacy*, pp. 44-54.

- **Tails (martie 2018)**

Tails.
https://tails.boum.org/

- **Tchabe și Xu (2014)**

Gildas Nya Tchabe și Yinhua Xu. 2014. *Anonymous Communications: A Survey on I2P*. CDC Publication.

- **Tenable Network Security (07.10.2016)**

I2P Outbound Connection Detection.
https://www.tenable.com/pvs-plugins/7170

- **The Tor Project (27.09.2009)**

Tor Partially Blocked in China.
https://blog.torproject.org/tor-partially-blocked-china

- **The Tor Project (2018a)**

Tor: Bridges.
https://www.torproject.org/docs/bridges

- **The Tor Project (2018b)**

Tor Metrics.
https://metrics.torproject.org/

- **The Tor Project (2018c)**

Tor: Pluggable Transports.
https://www.torproject.org/docs/pluggable-transports

- **Thomas Erdbrink (01.05.2018)**

Iran, Like Russia Before It, Tries to Block Telegram App. *The New York Times*.
https://www.nytimes.com/2018/05/01/world/middleeast/iran-telegram-app-russia.html

- **Timpanaro et al. (2015)**

Juan Pablo Timpanaro, Thibault Cholez, Isabelle Chrisment și Olivier Festor. 2015. *Evaluation of the Anonymous I2P Network's*

Design Choices Against Performance and Security. În *International Conference on Information Systems Security and Privacy (ICISSP)*. IEEE, pp. 1-10.

- **Timpanaro et al. (2012)**

Juan Pablo Timpanaro, Isabelle Chrisment și Olivier Festor. 2012. *A Bird's Eye View on the I2P Anonymous File-Sharing Environment*. În *International Conference on Network and System Security*. Springer, pp. 135-148.

- **Timpanaro et al. (2014)**

Juan Pablo Timpanaro, Isabelle Chrisment și Olivier Festor. 2014. *Group-Based Characterization for the I2P Anonymous File-Sharing Environment*. În *NTMS 2014 Conference and Workshops*.

- **Timpanaro et al. (2011)**

Juan Pablo Timpanaro, Isabelle Chrisment și Olivier Festor. 2011. *Monitoring the I2P Network*. Teză de doctorat. INRIA.

- **Winter și Lindskog (2012)**

P. Winter și S. Lindskog. 2012. *How the Great Firewall of China Is Blocking Tor*. În *The 2nd Workshop on Free and Open Communications on the Internet*. USENIX.

- **Xu (08.03.2016)**

Young Xu. *Deconstructing the Great Firewall of China*. ThousandEyes Blog.

- **Zamani et al. (2017)**

Mahdi Zamani, Jared Saia și Jedidiah Crandall. 2017. *TorBricks: Blocking-Resistant Tor Bridge Distribution*. În *International Symposium on Stabilization, Safety, and Security of Distributed Systems*. Springer, pp. 426-440.

- **Zantout și Haraty (2011)**

Bassam Zantout și Ramzi Haraty. 2011. *I2P Data Communication System*. În *Proceedings of ICN 2011, The Tenth International Conference on Networks*.

- **zzz (27.08.2011)**

Frequently Asked Questions. I2P Development and Discussion Forum. http://www.zzz.i2p/topics/969-proposal-auto-hidden-mode-for-certain-countries

- **zzz (Pseudonym) și Lars Schimmer (2009)**

zzz (Pseudonym) și Lars Schimmer. 2009. *Peer Profiling and Selection in the I2P Anonymous Network*. În *Proceedings of PET-CON 2009*, pp. 59-70.

- **zzz's I2P Statistics Website (2018)**

NetDB Statistics Index. http://stats.i2p